The Role of Cyber Security in the Technology Transfer of eHealth Applications

Luminița CRĂCIUN
National Institute for Research and Development in Informatics - ICI București
luminita.craciun@ici.ro

Abstract: The major changes in the field of health, determined by the evolution of the digital world, but also by other social factors (Covid-19 pandemic, the Russian-Ukrainian war, the increase in the incidence of drugs and car accidents, etc.) or natural factors (cataclysms) generate the need for a rapid technological transfer between eHealth software developers and healthcare professionals. The European Commission for Health constantly carries out studies to present the situation of digitization of the medical field in EU member countries, also proposing measures for those in which the pace of implementation of IT solutions is slower. In addition to this situation, the Commission emphasizes that it is necessary to take the the appropriate measures to avoid risks and protect personal data from cyber attacks and threats by ill-wishers, which can make it difficult to perform the medical act. This article highlights the fact that eHealth applications can be protected from attacks like phishing, ransomware, DDoS, malware, etc. if the technological transfer confirms the inclusion of cyber protection measures in the new product or if it is done with the help of blockchain technology.
Keywords: eHalth applications, technology transfer, eHealth cyber attacks, blockchain for eHealth.

INTRODUCTION

The fast pace of digitization determines the finding of quick solutions through which new technologies can quickly find their applicability in all fields of activity. If scientists focus on finding the most modern, useful and fast digital technologies to make people's lives and work better and more efficient, IT specialists must think of ways and solutions to put research results into practice in the shorter time.

The process by which the results of scientific research and technological innovations become accessible to the widest possible range of users is called technology transfer.

In a broader approach, technology transfer can be understood as a transshipment of knowledge materialized by new scientific discoveries, usually created and developed in research laboratories and/or academia, to society. This transfer of knowledge can be achieved, mainly, in the context of establishing mutually

https://doi.org/10.54851/v5i2y202306

beneficial collaborative relationships between research centers/institutes and the academic environment with the relevant industry. However, technological transfer can also be achieved through publications (scientific works, articles, books), during scientific conferences or through innovation patents.

As a rule, a successful technological transfer leads either to the creation of new products and services, or to the improvement of the quality and performance of the existing ones, including the improvement of manufacturing processes. That is why technological transfer, especially of digital technologies, is essential for the growth and maturation of both productive units and institutions in the sphere of social services, including those in the health sector as the reference area for this article. In this sense, the use of digital technologies in the field of health has radically transformed the vision of how to collect and use health data and information. The Covid-19 pandemic has made healthcare practically dependent on the data and information received from patients, and doctors have realized that the use of digital technologies to process this data leads to the transformation and efficiency of healthcare services. Without the transfer of digital technology, it would not have been possible for these institutions to keep up with the dynamics of technological developments or social changes. Through digitization, medical services have evolved so that they currently include services such as electronic health records, eHealth, mHealth, telemedicine, artificial intelligence, telecare, imaging, etc.

But, as in any other field, when implementing a digital technology transfer project in healthcare institutions, there are a number of risk factors, among which technological risk factors occupy a central place. The technological risk is associated with the lack of novelty and inadequacy of digital technologies to the specific features of institutions in the medical field, as well as the vulnerability of these technologies to the action of external factors, among which cyber security risks and threats occupy a central role.

This situation happens because the security of medical equipment based on digital technologies is an extremely important issue for the medical field. Cyberattacks can make it difficult to carry out and even stop healthcare activities, which could become fatal for patients' lives. In the future, these threats will not disappear, but will diversify in proportion to the evolution of digital technologies. Therefore, it is very important that these technologies are transferred to medical institutions by rigorously checking the protection they present against cyber attacks. In this way, by transferring to medical units IT systems protected against cyber attacks, there will be the certainty that medical devices, data and, most importantly, patients are also protected.

Considering these aspects, this article analyzes some characteristics that digital technologies should present in order to reduce their vulnerabilities to cyber attacks and to be successfully transferred to institutions in the medical field. In this context, the present paperwill show what the main cybersecurity challenges for eHealth applications are and why technology transfer plays an important role in reducing them.

TECHNOLOGICAL TRANSFER – CATALYST FOR THE DEVELOPMENT OF DIGITAL TECHNOLOGIES FOR EHEALTH SERVICES

The concept of *technological transfer* registers several interpretations. On the one hand, the concept refers to a material component – products, equipment, layouts, techniques or processes – and to an informational one – the totality of knowledge in fields such as management, marketing, production or quality control (Crișan et al., 2018). The material component can be divisible or not, leading to state transformations of the two partners of the transfer (Drouvot & Verna, 1994): *the source* which conducts intensive research to identify needs in a certain field, creating an innovative product, and *the receiver* (public institution or private partner) willing to implement the

research results. However it should be noted, that both *the source* and *the receiver* are entities with legal personality (institutions, firms, companies, associations, agencies, organizations, etc.) that are subject to the rigors of the legal norms regarding the ownership of the new product.

Studies on technology transfer have highlighted the link between technology and technological knowledge. It is obvious that a new product comes with a technical sheet that presents the innovative elements, the details regarding the ways of use, the protection and safety measures at work, so that the user can use it in the fullness of its functions. Integrating the product into the receiver's activity means technological know-how, which would involve going through some stages of previous preparation. For this, the organization must motivate employees to acquire new information and skills, so that a technological transfer of innovative products is quickly integrated into the activity.

The exchange between the two partners of the technology transfer process causes independent and/or reciprocal changes in the source and recipient organizations, as a result of the effort to integrate the new product. Also, the permanent determination to update the information regarding the development of its performances is required.

As a process, technological transfer falls to the company or institution holding the research results and which, through various promotion methods, seeks the best exploitation of its products, after they have passed the homologation stage. The legislation in Romania regarding the protection of inventions (Law 64/91 on patents and inventions – updated in 2014, Law 83/2014 on service inventions, Law 8/1996 on copyrights – updated in 2023) constitutes the legal framework for achieving the transmission of rights from the owner to the beneficiary. The initiative to capitalize on the innovative product can also be mediated by independent technological transfer centers, specialized precisely for finding partners with high potential for acquisition and integration into their own activity.

In the case of IT applications, the technology transfer process must be accompanied by the presentation of personal data protection and network and system security solutions. European and national legislation requires the creators of digital applications to include, from the development process, such methods against attackers and unauthorized access. Respect for privacy and personal data are fundamental rights in the EU, so they must be protected.

The field of health is one in which innovation is a permanent concern due to the interest of specialists in finding solutions to eradicate some diseases, to improve some chronic conditions and, finally, to increase the average life of people. Here, in addition to the practitioners who come into direct contact with those in pain, there are also a pharmaceutical industry concerned with the innovation of medicines to offer solutions to solve complex health problems and a medical technology industry where studies are focused on creating the best performing devices for health investigation. In addition to these, IT specialists expressed their interest in facilitating the monitoring, investigation and recording of patients' vital parameters, as well as in offering ameliorative solutions, creating the *eHealth branch*.

In the view of the European Commission, *eHealth* brings together tools and services that use ICT (information and communication technologies) for the prevention, diagnosis, treatment and monitoring of patients, facilitating the development of quality medical care. The field of eHealth includes the exchange of information between patients and medical personnel, the creation of the medical file with the results of the investigations made and the treatment given, telemedicine services, portable devices for monitoring patients, software for appointments or for various interventions, robotic surgery, etc.

eHealth applications come to the aid of doctors and medical staff as well as patients, managing to improve their access to health services and provide them with the possibility of specialized medical care. Access to the

new eHealth applications is achieved through electronic devices (smart watches, smart bracelets, mobile phones, laptops) connected to the Internet (Nicolau, 2022). These come to facilitate the work of doctors and medical personnel, thus streamlining medical consultation appointments and eliminating waiting time or ensuring the storage of data related to patient investigations and treatments offered. In Romania, applications such as *xCapture* from Netpulse, a technology company focused on fitness and cardiac monitoring, are highly sought after; the *VitalSnapValidic* system from Validic, a leader in digital health platforms, which connects the family doctor with the pacients by means of a simple phone that can take photos; Android health apps: White Noise Lite, for people who have sleep problems, Instant Heart Rate, approved by the European Health Commission, which measures heartbeats, etc.

The penetration of these applications into the market is a challenge for the medical staff oriented towards investigating, advising the sick and finding solutions to remedy their health condition, but also a benefit due to the real-time monitoring of the investigations carried out by the patients. The use of *eHealth* applications and platforms allows dialogue between the doctor and the patient, between doctors of different specialties and the family doctor, precisely for the purpose of providing quality medical services and improving the patient's health.

The complexity of the human genome, as well as the diversity of rare and/or degenerative diseases, require the collaboration of medical specialists from various branches of medicine. That is why interest in eHealth applications is growing, and technology transfer is the fastest way to make digital tools available.

CYBER SECURITY CHALLENGES IN TECHNOLOGY TRANSFER OF EHEALTH APPLICATIONS

Even if the digital environment makes available newer and more powerful tools, the design and then use of eHealth applications require the implementation of security measures, so that the information circulated is protected from cyber attacks. In fact, as it has been previously mentioned, IT specialists take into account, from the design of the applications, the security measures possible at the time to avoid or minimize the effects of possible *cyber attacks* and data protection. It should be noted that the IT field is very dynamic, thus the protective measures can anticipate possible risks, but cannot cover all of them.

In the study developed by the European Union Agency for Cyber Security 2023 (ENISA) entitled *ENISA Threat Landscape: Health Sector,* the main threats targeting the eHealth field are highlighted, as follows: Ransomware, Data-related Threats, Intrusion, DoS/DDoS/RDoS, Supply Chain Attack, Malware, Errors, Misconfigurations, Security Practice, Social Engineering threats (see Figure 1).

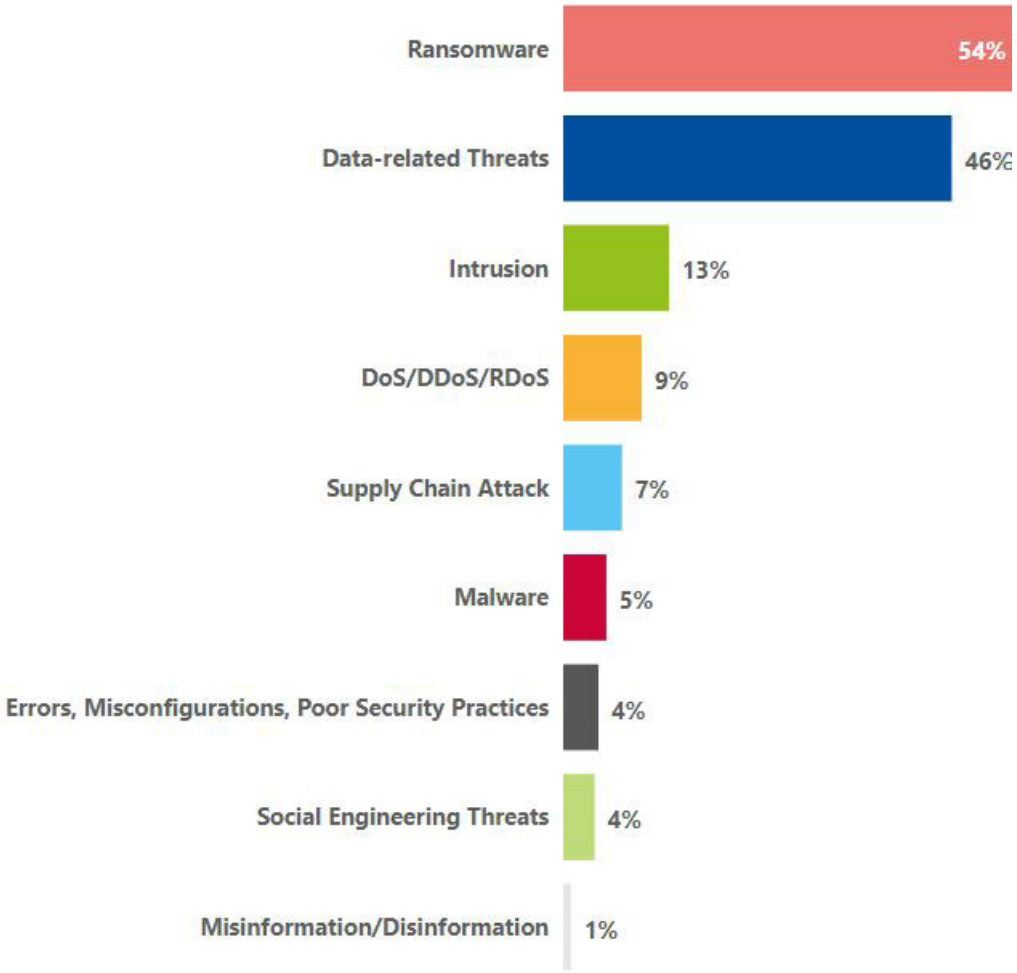

Figure 1. *Threats in the health sector (January 2021 to March 2023) (ENISA, 2023)*

The study covers the period January 2021-March 2023 and provides an overview of cybersecurity threats to the healthcare sector in the European Union, providing information on trends and patterns to drive prioritization of actions and decisions. However, it should be noted that the data used for the analyzes carried out in this report refer to a significant part of the period of the Covid-19 pandemic. During this time, the healthcare sector started to become one of the main targets of cyber attackers. Thus, there was an increase in cases of data leakage from medical systems and Covid-19 testing laboratories in many EU countries, during the pandemic and, over time, cyber attacks multiplied, targeting also other elements of the European medical systems.

As the conclusions of the report show, in the analyzed period, the number of cyber security incidents increased significantly in the European health sector and the main threats were ransomware and unauthorized data access. The authors of the report believe that this trend will continue as cybercriminals make significant financial gains by threatening both healthcare organizations and patients with the disclosure of sensitive data, namely personal data of patients.

Another category of incidents concerned the exploitation of vulnerabilities in health systems. Among them, vulnerabilities in the supply chains of healthcare providers, as well as those presented by the software or hardware used in healthcare systems, were one of the main causes of cyber security incidents.

Another important aspect of cyber incidents in the field of health at the European level is related to geopolitical developments, especially the Russia-Ukraine war, which brought new aspects to the approach of cyber security and hacktivist activity. The report shows that early 2023 saw an increase in Distributed Denial of Service (DDoS) attacks by pro-Russian hacktivist groups against hospitals and health authorities, and this trend is expected to continue, although the actual impact of these attacks remains relatively low.

However, when comparing these conclusions with those published by ENISA in their annual report – *ENISA Threat Landscape 2022*, in November 2022, it can be seen that the health sector is not the preferred target of cyber attackers (see Figure 2).

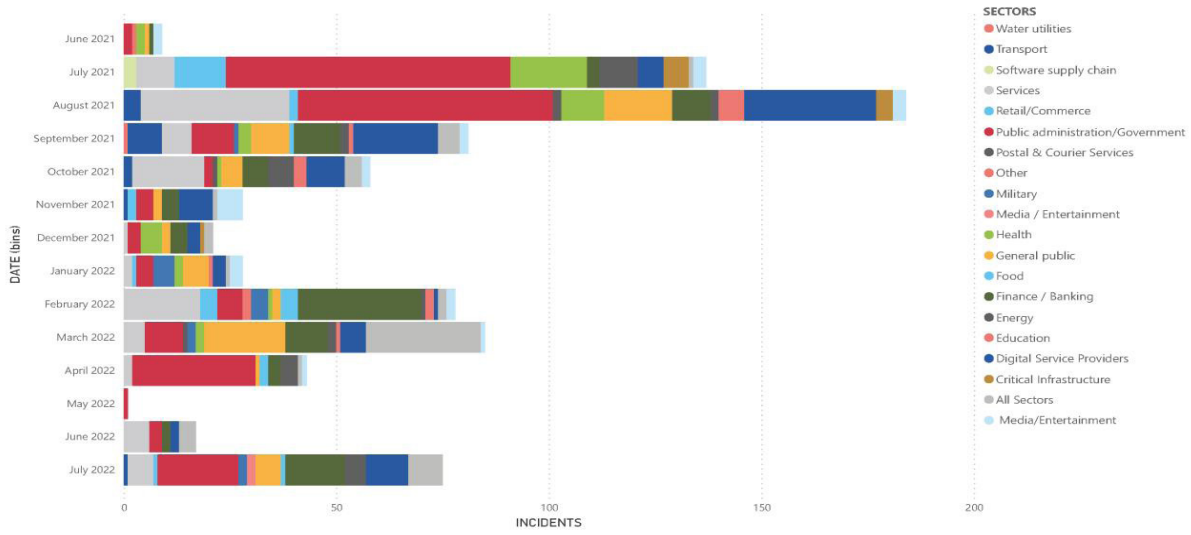

Figure 2. *Security incidents in various sectors of activity (ENISA, 2022)*

However, the risk of affecting critical healthcare infrastructure, as well as the multitude of personal information circulated through eHealth applications and platforms, prompt the need for protective measures.

The concern of the European Health Commission is to make possible, under security conditions and in compliance with national and European legislation, the transfer of health files of patients who travel, work or emigrate in the European space, for a quick solution of problems that may arise (ENISA, 2022). If they are not protected, eHealth applications can represent the source of information that unauthorized persons can access from the desire to use them for other illegal purposes (e.g., access to bank accounts).

Moreover, the study *eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the EU Lot 1 - Interoperability of Electronic Health Records in the EU (2020)* carried out by the European Commission DG Communications Networks, Content & Technology (2021), based on surveys taken place during the Covid-19 pandemic, presents the extent to which the EU member states are prepared for the transfer of data through digital technologies (see Figure 3).

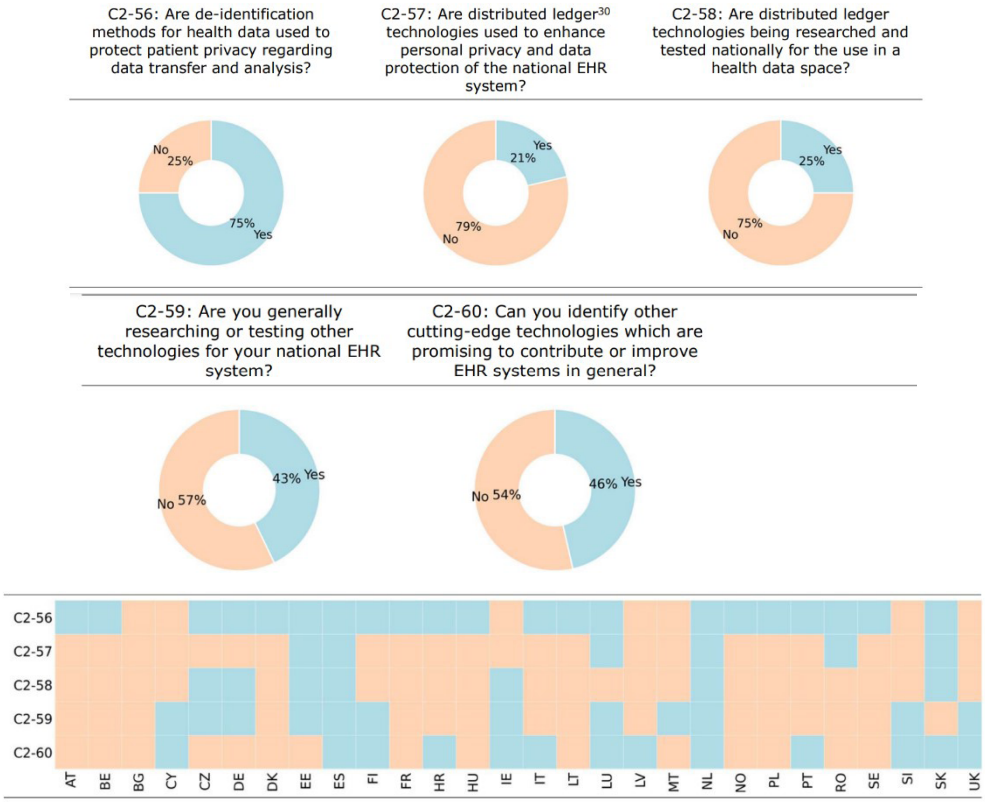

Figure 3. *Analysis of the European Commission regarding the stage of implementation of eHealth solutions in the EU member states (European Commission DG Communications Networks, Content & Technology, 2021)*

Romania stands out for having introduced distributed ledger technology (DLT) or blockchain to enable better data security. This technology is currently revolutionary in the way it collects and distributes information that applies to both static (recorded in documents) and dynamic data (transactions).

CYBER SECURITY MEASURES USED FOR TECHNOLOGY TRANSFER OF EHEALTH APPLICATIONS

Collaboration between eHealth application developers, healthcare providers, and regulators is crucial to ensure cybersecurity in technology transfer. Besides, it is the legal framework that establishes the steps of the procedure after obtaining the homologation certificate. However, before starting the steps to carry out the transfer, a code audit is necessary that can guarantee the receiving partners that the product also includes measures aimed at data protection. The implementation of cybersecurity standards and regulations, as well as the exchange of best practices between parties, can help create a secure environment for the technology transfer of *eHealth* applications.

One of the cyber security measures used for the technological transfer of eHealth applications is the encryption of medical data. This can ensure the protection of stored information, making it unreadable for unauthorized persons. Moreover, theorists have mentioned and enumerated a set of requirements that eHealth applications should fulfill. The study *Reusable security requirements for healthcare applications* lists them (Tîrziu & Gheorghe – Moisii, 2018), showing that, in order for them to be used in cyber security conditions, it is necessary to identify and verify the identity of all users before allowing them access to existing resources. Also, the checking of the authorization level of users before accessing personal data, thus ensuring the protection of data as long as it is stored, the

detection of unauthorized manipulation of the transmitted data, the protection of all sensitive personal data against unauthorized access, the logging of security incidents, such as failed or unauthorized authentication attempts to access services, the ensuring of multiple levels of security, the existence of a patient log that must show who added content, e.g. through electronic signatures, are among these requirements.

Another way to reduce the risk of unauthorized access to medical information is to implement strong authentication methods, such as two-factor authentication (2FA) or multi-factor authentication (MFA). Two-factor authentication involves using two different elements to confirm a person's identity, such as a password and a code generated by a mobile app or text message. Thus, even if someone obtains the password, he/she cannot access the account without the additional factor. Multi-factor authentication extends the concept of two-factor authentication by adding additional factors such as fingerprint or facial recognition. These additional methods increase the level of security, because it is more difficult for an attacker to obtain or imitate these unique characteristics.

Last but not least, periodic verification, auditing and evaluation of *eHealth* systems and applications can lead to the identification of potential vulnerabilities and ensure their timely updating and remediation. Verification refers to the careful examination of *eHealth* systems and applications through an in-depth analysis of source code, configurations and security policies to identify potential problems or weaknesses that could be exploited by attackers. Auditing consists in the detailed examination and evaluation of *eHealth* systems and applications to determine whether they comply with established security standards and policies. The audit can be carried out internally or by involving independent third parties who analyze and evaluate the system according to security requirements and applicable regulations. This activity is carried out before sending the product for approval and the technological transfer, precisely to offer potential applicants (recipients) a product that complies with the legal framework regarding the protection of personal data. Finally, periodic assessment consists in constantly reviewing and updating *eHealth* systems and applications to ensure that they remain secure and compliant with applicable standards and regulations. This process involves regularly reviewing security policies and procedures, updating software and security patches, and actively monitoring cybersecurity activity and incidents.

Also, to avoid any cyber security incident, eHealth applications must be accompanied by user guides for both medical staff and patients, as well as user training/preparation for the successful use of the product (Alexandru, 2022).

A novelty in the context of data security is the blockchain technology that provides the secure recording and storage of transactions and data in a distributed and immutable ledger. This offers a number of advantages in terms of cyber security, such as advanced encryption, decentralized authentication and data integrity verification. As summarized by Stanimir (2018):

„This technology ... could contribute to the automation and efficiency of chains determined by processes, permissions and input of documents ... processes that certify ownership, medical records or that of insurance of an asset, all are under the sign of the impact of blockchain" (p.577).

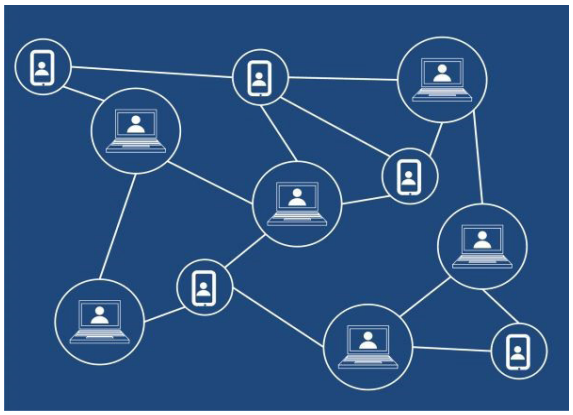

Figure 4. *Blockchain technology (Rivera, 2018)*

In the context of the technology transfer of *eHealth* applications, the use of blockchain technology can bring a number of improvements in the security of medical data. This can provide a greater level of transparency and secure control over access to medical information, eliminating the risk of unauthorized data modification or deletion. In addition, the use of blockchain technology can ensure a secure digital identity for patients and healthcare professionals, creating a decentralized system of authentication and authorization and eliminating the risk of identity theft and/or unauthorized access to medical data.

Blockchain can also help increase trust between parties involved in the technology transfer of *eHealth* applications, such as developers, healthcare providers, and patients. Through this technology, a decentralized and secure system of sharing medical data can be created, ensuring that the information is authentic, verifiable and confidential.

Another important advantage of using blockchain is the easy auditing and verification of shared data, because it creates a transparent and verifiable system where any change or access to medical data can be recorded and verified. In this way, the integrity and confidentiality of medical information is ensured. They cannot be changed or deleted, and their accuracy is guaranteed.

The use of blockchain technology can also ensure the security of financial transactions in the case of *eHealth* applications. Thus, smart contracts and decentralized payment mechanisms can be created, eliminating the risk of fraud and manipulation of financial transactions.

Last but not least, blockchain can also be used to monitor and detect cyber attacks in the technology transfer of *eHealth* applications, facilitating the creation of threat detection and event recording systems, ensuring that any attempted cyber attack can be identified and countered in a timely manner.

Being a novelty in the digital field, blockchain technology is used, at the moment, with priority in the United States, but there is also a special interest in Great Britain, France, Switzerland, the Netherlands and Germany.

An example of using blockchain technology in the field of eHealth is the MedRec project of specialists from Massachusetts Institute of Technology – MIT, that uses a system based on Ethereum software to connect healthcare providers who are allowed to share data/information medical facilities in secure conditions, and the patients. Thus, the possibility of connecting patients and medical staff is created through the use of specialized information.

Also, via Ethereum, the Gem Health Network project uses blockchain technology to create a secure and interoperable network for healthcare data and applications. Thus, it facilitates the safe and transparent transfer of medical data between the various entities in the health system, including patients, medical service providers and those in the field of insurance. Gem Health founder and CEO, Micah Winkelspecht, argues that blockchain will enable the creation of a robust and resilient healthcare ecosystem with industry-wide workflows that involve moving data between multiple parties.

Blockchain technology is a novelty in the digital environment and, therefore, there is still reluctance or inexperience in introducing it in areas that process a lot of data and personal information. But the fast pace of digitization will require the use of the most effective solutions to facilitate access to information useful in solving various problems, including those from the health area.

CONCLUSIONS

Technology transfer is a process occurring between two partners who must mutually benefit from advantages (material, financial, professional development, etc.). In Romania, the current interest in the training of specialized experts for this activity is contained in the National Plan for Research, Development and Innovation 2022-2027, where there is a subchapter dedicated to technology transfer regarding the purpose and types of projects proposed for financing. This is because Romania is in a higher stage of development, imposed by the innovations in the IT field,

which requires changes, transformations and, above all, digitization in various fields, including the health area. That is why collaboration between IT specialists and medical personnel is necessary to ensure the training of working groups capable of using eHealth applications.

The main reason for the introduction of digital technologies in the field of health is the efficiency of working time. This means speed in scheduling patients for consultation, in processing analyses, in interpreting the results to establish a diagnosis, correlating all the information related to the patient's health status, proposing the best treatment, quickly finding solutions to solve health problems.

For the efficient use by the various categories of beneficiaries (medical staff, patients, insurers), but also in maximum safety of medical data and information, eHealth applications must include data encryption technologies and block unauthorized access to the medical file of the patient. In addition to known security measures, the use of blockchain seems to be the best solution for securing data, confidentiality and integrity of medical information in patient-doctor communication or between medical specialists (family doctors, specialist doctors, recovery doctors, etc.).

Being a novelty in the IT field, it is necessary to organize training courses for health IT specialists to ensure the circulation of medical information between the various nodes of the blockchain network, under conditions of maximum cyber security.

REFERENCE LIST

Alexandru, A., Ianculescu, M., Giura, I. E. & Pop, F. (2022) Managing Cybersecurity Threats for Seniors' Digital Needs Using Age-Friendly Remote Healthcare Monitoring Model. In: *2022 E-Health and Bioengineering Conference (EHB), 17-18 November 2022, Iași, Romania.* pp. 1-4. doi: 10.1109/EHB55594.2022.9991316

Crișan, E., Pop, M., Salanță, I., Nistor, R., Beleiu, I. & Mihăilă, A. (2018) *Technology transfer – for businesses and universities [Transferul tehnologic – pentru întreprinderi și universități].* Cluj-Napoca, Risoprint.

Drescher, D. (2017) *Blockchain Basics: A Non-Technical Introduction in 25 Steps.* Frankfurt am Main, Apress.

Drouvot, H. & Verna, G. (1994) *Technological development policies – The Brazilian example* [Les politiques de developpement technologique – L' exemple brasilien]. Paris, Editions de l'Iheal. https://books.openedition.org/iheal/1649 [Accessed 9th September 2023].

Nicolau, D., Bica, O. & Băjenaru, L. (2023) Data Security Approach in Remote Healthcare Monitoring. R*omanian Cyber Security Journal*. 5(1), 45-55.

Popescu, M. (2016) *Innovation management [Managementul inovării]*. Brașov, Transilvania University Publishing House.

Puchiu, R., Stoian, M. & Foca, M. (2018) *Digital Romania. Concepts and operational tools* [România digitală. Concepte și instrumente operaționale]. Bucharest, Club Romania Publishing House.

Rivera, M. (7 January 2018) *Blockchain Technology In Education: How The Latter Can Be Disrupted. eLearning Industry.* https://elearningindustry.com/blockchain-technology-in-education-latter-can-disrupted.

Tapscott, D. & Tapscott, A. (2021). *The blockchain revolution. About how the technology behind bitcoin is transforming money, business and the world [Revoluția blockchain. Despre felul în care tehnologia aflată la baza bitcoinului transformă banii, afacerile și lumea]*. 2nd ed. Bucharest, ACT & Politon.

Tîrziu, E. & Gheorghe - Moisii, M. (2018) Quality Characteristics of eHealth Applications [Caracteristici de calitate ale aplicațiilor eHealth]. *The Romanian Journal of Informatics and Automation* [Revista Română de Informatică şi Automatică]. 28(2), 29-40.

The European Commission DG Communications Networks, Content & Technology. (2021) *eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the EU Lot 1 - Interoperability of Electronic Health Records in the EU (2020) SMART 2019/0056.* https://digital-strategy.ec.europa.eu/en/library/interoperability-electronic-health-records-eu [Accessed 25th August 2023].

The European Union Agency for Cybersecurity (ENISA). (2022) *ENISA Threat Landscape 2022 July 2021 to July 2022.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [Accessed 11th September 2023].

The European Union Agency for Cybersecurity (ENISA). (2023) *Health Threat Landscape. January 2021 to March 2023.* https://www.enisa.europa.eu/publications/health-threat-landscape [Accessed 25th August 2023].