Medicine and Law

World Association for Medical Law

Volume
42

Number 2
June 2023

Published by William S. Hein & Co., Inc.
Getzville, New York

ISSN 0723-1393

UNIVERSITY OF HAIFA

International Center for Health, Law and Ethics
University of Haifa, Law Faculty, P.O.Box 6451
Haifa 31063, Israel

Med Law (2023) 42:2:481-494

Medicine and Law
World Association for Medical Law

Medical Regulation

FEATURES OF ADMINISTRATIVE AND LEGAL SECURITY AND CONFIDENTIALITY IN MEDICAL INFORMATICS

Leontii Chystokletov*, Oleksandra Khytra, Valerii Shyshko***, Nataliia Blok****, Mariana Tarnavska******

Abstract: The aim of this article is to consider patient safety strategies in current diagnostic and treatment environments, in medical informatics. The study uses scientific knowledge methods, approaches and techniques – both general scientific and special, including: dialectical, historical and legal, logical, system analysis, statistical, system-structural, comparative-legal, logical-semantic, formal-legal, and more. The decisions' development and adoption, in security in medical informatics, should be organised in conjunction with public authorities whose mandate includes security preservation in information systems. Security and privacy basics in medical informatics should be studied separately from society, state and global information security systems and consider their mutual determinacy and interaction.

Keywords: Patient Safety Strategies; Global Health Protection; Medical Information; Information Technology; Healthcare Information System

* **Department of Administrative and Informational Law, National University "Lviv Polytechnic", 79000, 12 Stepan Bandera Str., Lviv, Ukraine. leon.chystokletov@ukr.net**

** **Department of Administrative Law and Administrative Procedure, Lviv State University of Internal Affairs, 79000, 26 Horodotska Str., Lviv, Ukraine. khytraoleksandra@yahoo.com**

*** **Department of the Theory, Constitutional and Private Law, Lviv State University of Internal Affairs, 79000, 26 Horodotska Str., Lviv, Ukraine. valer.shyshko@hotmail.com**

**** **Department of Civil Law and Procedure, National University "Lviv Polytechnic", 79000, 12 Stepan Bandera Str., Lviv, Ukraine. nataliia_blok@yahoo.com; mari.tarnavska@meta.ua**

Introduction

Ensuring safety and confidentiality is important for global health protection. The process to reduce danger levels from medical actions can be represented as a four part problem: formalisation of task, terms, and classifications; quality assessment of strategic medical care issues; assessment of complication risks during treatment, and their monitoring and hazard identification; and error with identification and analysis of diagnosis and treatment. The vast array of medical information, the lack of preservation control, and low technical reliability raise serious concerns about information preservation. During systems operation, information is vulnerable to destruction and unauthorised use. The different components, operations, resources and high number of facilities creates an attractive environment for intrusions and unauthorised actions[1].

Citizens' rights, rights of legal entities and the state to freely receive, disseminate and use information, and the need to protect confidential information and intellectual property are all important within healthcare. The role of information security role in healthcare is growing considerably[2,3]. There are many known cases of medical information disclosure or perversion which have led to unintended consequences, even to patient suicide[4]. Security and confidentiality concerns are highly relevant[5].The aim of this article is to conceptualise patient safety strategies for medical information in diagnostic and treatment environments. Due to the complex nature of the topic, legal, information technology and medical literature sources were utilised. Security and confidentiality issues in medical informatics have been dealt with by such

1 B.A. Kobrinsky. "Information medical systems integration Prospects and ways". *Doctor and Information Technologies* (2009), 4: 4-11.
2 J.F. Almadani and A.P. Putera. "Legal liability of doctors on the disclosure medical secrecy for Covid-19 patients in the pandemic era". *Jurnal Hukum Prasada* (2021), 8(1): 8-20.
3 O.M. Yaroshenko, V.M. Steshenko, H.V. Anisimova, G.O. Yakovleva and M.S. Nabrusko. "The impact of the European court of human rights on the development of rights in health care". *International Journal of Human Rights in Healthcare* (2021). DOI: 10.1108/IJHRH-03-2021-0078
4 F. Pochard, M. Grassin, N. Le Roux and C. Hervé. "Medical secrecy or disclosure in HIV transmission: A physician's ethical conflict". *Archives of Internal Medicine* (1998), 158(15): 1716-1719.
5 O.V. Prudnykova, V.M. Pyvovarov, O.V. Fedosova, O.A. Stasevska and O.V. Umanets. "European court of human rights as a guarantee of observation the medical secrecy". *Journal of Forensic Science and Medicine* (2021), 7(4): 145-151.
6 B.A. Kobrinsky. "Information medical systems integration Prospects and ways". *Doctor and Information Technologies* (2009), 4: 4-11.

domestic and foreign scientists such as B.A. Kobrinsky[6], V.S. Kolomoytsev & V.A. Bogatyrev[7], K.J. Chung et al[8] and others.

Security and privacy solutions involve improving the process structure and care outcomes. This involves: physician skills analysis; equipment and nursing staff provision; assessment of organisation and funding conditions (the structure quality); assessment of diagnostic and treatment activities (process quality); the outcome (quality analysis).

Methods

The methodological basis of the study was scientific knowledge methods, approaches and techniques including: dialectical, historical and legal, logical, system analysis, statistical, system-structural, comparative-legal, logical-semantic and formal-legal.

This study also used legal hermeneutic philosophical arsenals, ontology and axiology. In particular, the historical-legal method was used to understand legal formation and development, and to understand and research the preconditions of personal information rights formation in public health services. The system-structural method allowed consideration of the internal structure of information security and privacy in medical informatics as a complex social and legal phenomenon, as well as support in determining the legal support system study methodology for information security. The structural-functional method made it possible to investigate the role of decision-making on security and confidentiality in medical informatics. The classification method was used to comprehend information security threats in health care, highlighting social groups with certain specific characteristics that entail that their information be held.

Results and Discussion

The formation of information risks can be tracked upon request. The Google word selection service allows you to receive statistics by parameter. According to the demand for secure information it is necessary to define a general list of information podcasts, which during such periods will be in high demand,

7 V.S. Kolomoytsev and V.A. Bogatyrev. "Multilevel protected access structural organization choice effectiveness and justification Estimation to external network resources". *Information and Space* (2015), 3: 71-79.

8 K.J. Chung, J. Kim, T.K. Whangbo and K.H. Kim. "The prospect of a new smart healthcare system: A wearable device-based complex structure of position detecting and location recognition system". *International Neurourology Journal* (2019), 23(3): 180-184.

and, therefore, require additional protection. In particular, the publication News Guard[9] showed an overestimation of the level of concern by some media, due to different social behaviours on the site. This creates an increased risk of changing social behaviour and social access, but also opens up new opportunities for phishing attacks such as: emails with malicious attachments; proposal to install malicious attachments (for example, tracking social contacts); false information portals to access classified information; access to remote phase video conferencing (Skype, Teams, Zoom, etc.)[10].

It should be noted that the multicomponent sphere uses input data from the results of the previous blocks, which is not always strictly defined. More useful would be to use cyclic operations between modules/participants systems, and the participants of the modules themselves, who are equalised in rights and responsibilities based on their economic role. In particular, an example can be brought from the exchange experience, when a sharp increase in demand for remote services communication, in particular zoom, led to a jump in investor demand on the shares of this company, while investors bought shares of Zoom Technologies, increasing the capitalization of the company Pania by 47000%[11].

In the Ukrainian information system, there was an increase in consumption of state information resources. In domestic intelligence, there was an increase in requirements of state information resources, which in March 2020 showed failures, and some communication services decided to block high-definition video[12]. In this case, we can talk about the correlation of the level of biological and informed security. In this case, the issue of information security, which is affected by the State Program "Information Society" is seen in a new way, which requires institutional intervention measures and adjustments to create and maintain a balance of information security during biological threats.

Comparing the emergence of prescriptive (prohibitive) acts with the information agenda, allowed us to conclude that the latter is left open and society's requests

---

9 A.A. Sogiainen. "Handling information constituting medical secrecy Peculiarities". *Law in Armed Forces* (2017), 3: 26-31.

10 A. Kolotik. "Current state of social security for employees of the National Police of Ukraine: A literature review". *Scientific Journal of the National Academy of Internal Affairs* (2022), 27(4): 52-61.

11 J. Perlow. "Coronavirus misinformation spreading fast: Fake news on COVID-19 shared far more than CDC, WHO reports". (2020). Retrieved from: https://www.zdnet.com/article/coronavirus-misinformation-is-increasing-newsguard-finds/

12 Managing the information security impact of COVID-19. (2020). Retrieved from: https://home.kpmg/xx/en/home/insights/2020/04/managing-the-information-security-impact-of-covid-19.html

for ensuring economic security in this aspect are not observed. Society's requests are wider than explanatory documents. Economic activity of small business agents was not prepared, and no ways were proposed for information stabilisation of the situation, as evidenced by peak information requests during various periods of the pandemic[13]. Development of action scenarios for businesses during biological threats, or the correlation of information flows, can become an addition to State programs in order to prevent a sharp reduction in the number of registered small and medium-sized business entities.

Such an agenda for providing information security of economically active subjects can be to develop scenarios for small and medium-sized businesses in the presence of external threats (biological, informational, relatives, etc.). For example, it is necessary to determine the possibility of working enterprises when changing external conditions. Enterprises producing textile products can be retrained for the production of medical products (masks, gowns, etc.). Catering places can provide people with food and expand their assortment. The development of advanced training courses for personnel to change activity, and development of software for ensuring the economic security of citizens through providing information. Developing the availability of information flows for SMEs to reduce economic risks and to prevent an increase in the risks of losing financial resources.

These activities should lead to a decrease in information risks in national security systems in the current biological threat. The turbulent space associated with the implementation of external threats requires the development of information flows in order to prevent a decrease in the quality of life and economic activity. In the future, this will allow adjustment of the correlation for information flows to reduce information risk and economic security during periods of external threat. The actual reduction is a decrease in the total number of events to a sufficient level and will normalise operation of any system after interference with its operation.

With the advent of digital medical records, and the transition to electronic document management, there is an alienation of medical records from their source. This problem has been exacerbated by the transition to eHealth, which

13 G. Çera. "Europe's Economic Pandemic Shock: How EU Economies Endured the Effects of COVID-19 Restrictions". *European Chronicle* (2022), 7(4): 35-43.

includes a person-centred approach to patient records that involves each individual's health data integration in specialised data centres at processing different levels[14].

The complexity of solving medical information security problems is characterised by the following factors: the transition to paperless technology requires legal legitimacy through digital means; medical information systems require information security at the access delimitation level; the electronic documents require security at the content concealment level and, in some cases, unauthorised distribution prevention; high demands on the information and data sources authenticity due to geographical distribution; high requirements for software integrity (system and application), database management systems and electronic documents (reference, statistical, reporting)[15].

Medical informatics is a complex spatially distributed system consisting of local subsystems (information nodes) with software and hardware to provide connection and interaction with a wide range from the information services field to geographically remote users. In other words, it is an organisational and technical system that implements information technology and provides hardware, software and support other types, as well as appropriate personnel[16].

Protection and privacy in medical informatics depend on the following characteristics:

1. Categories of information processed in the medical information system.

2. The information highest classification.

3. The overall structure and composition (list and composition of equipment, hardware and software, users, data and their links, configuration and architecture features, etc.).

4. Medical information system type (single-user or multi-user system, open network, single- or multi-level system, etc.).

---

14 O.V. Petryshyn and O.S. Hyliaka. "Human rights in the digital age: Challenges, threats and prospects". *Journal of the National Academy of Legal Sciences of Ukraine* (2021), 28(1): 15-23.

15 E. Berge and F. van Laerhoven. "Governing the commons for two decades: A complex story". *International Journal of the Commons* (2011), 5(2): 160-187.

16 B.H. Weston and D. Bollier. *Green governance: Ecological survival, human rights, and the law of the commons*. (New York: Cambridge University Press, 2013).

5. The main information arrays and flows volumes.
6. The procedure duration for resuming operability after failures.
7. Means availability to improve reliability.
8. Technical characteristics of communication channels (bandwidth, cable lines types, communication types with information systems and users' remote segments, etc.).
9. Health information system component's territorial location, their physical parameters, etc.
10. The other special operating conditions presence, etc[17].

From the information protection viewpoint, typical system components are regarded as protection objects. These include: information protection system users and personnel workstations; communication facilities components (communication components); information protection system auxiliary elements; different functional purposes computers.

Medical protection information system workstations for users and staff. can be distinguished by the following types: terminals – display (not programmed) type user workstations with information visual display; workstations – user workstation (a personal computer) that can operate in the information exchange mode with the server as well as in an autonomous mode; operator's workplace designed for server maintenance; programming workstation designed for program renewal; an administrator workstation designed to manage and control the information protection system some resources use (network administrators, database administrators, security services)[18].

Communication facilities components (communication components): cross-network bridges (gateways, packet communication centres, communication computers) – elements that ensure several data transmission networks connection or the same network several segments that have different communication protocols; communication channels to communication nodes; communications equipment – modems (modulator-demodulator), which

17 V.I. Kalinichenko. "Medical care management creating an integrated system Necessity". *Physician and Information Technology* (2004), 2: 3-9.

18 E. Gibson. *Health information: Confidentiality and access.* (Ontario: LexisNexis Canada, 2011).

perform the digital data conversion into electrical signals for transmission over communication lines and the reverse conversion when exchanged between remote computers; communication equipment such as a data transmission multiplexer that interfaces several sources (e.g., several computers) for the information transmission over a single communication channel; individual and communication channels[19]. Supporting security elements can also be distinguished: premises, server rooms; rooms containing data pre-processing devices; data carriers' storage; documents repositories in paper form; offices for the information protection system users and personnel.

Different functionality computers: central computer (server, mainframe) that performs the information processing basic procedures in the medical protection information systems; server designed to perform the storage functions, data printing, network workstations service, etc.; computer with gateway functions, a bridge between network structures[20].

Lack of elementary technical control over medical information array means reliability, safety, and relatively low-level serious concerns in ensuring information safety. During the operation of protection systems, the information accumulated and processed is vulnerable enough to be destroyed and misused. The protection systems distinct components, operations, resources, and facilities creates a very attractive environment for intrusions and unauthorised actions' all kinds[21].

The main problems arising in protecting information can be distinguished: preventing information leakage, theft, loss, and forgery; preventing threats to person, society, and state information security; preventing information destruction, modification, copying, and blocking unauthorised acts. Also, preventing illegal interference in different forms and documented information use the legal regime as a property object to protect the citizen's constitutional rights to personal privacy and personal data confidentiality held in information systems[22]. This is also used to maintain medical secrecy, documented

19 Sh.G. Seidov. *Information processes in the globalization conditions*. (Penza: The Penza State University Publisher, 2008).

20 Freedom of Information and Protection of Privacy Act, RSA 2000, c F-25. (2020). Retrieved from: https://www.canlii.org/en/ab/laws/stat/rsa-2000-c-f-25/latest/rsa-2000-c-f-25.html#document

21 B.A. Kobrinsky. "Information medical systems integration Prospects and ways". *Doctor and Information Technologies* (2009), 4: 4-11.

22 V. Tymoshenko and L. Makarenko. "Political and legal guarantees of human and civil security". *Law Journal of the National Academy of Internal Affairs* (2022), 12(4): 9-16.

information confidentiality under applicable law and to guarantee subject rights in information processes and the information systems, technologies and their supporting means of development and application[23].

At present, personal computers are used to access and protect data. This approach expends considerable effort to organise protection for information that is processed using inexpensive hardware. When users have access to several servers and are allowed to log on remotely, protection is so complex that it becomes a challenge even for large medical institutions[24]. The most common means of information leakage are: data carriers and document theft from information systems; copying information onto a personal computer; unauthorised connection to equipment and communication lines; electromagnetic emissions interception during data processing[25].

In addition to the above, there are other hazards. For example: a system programmer breaches security, secures login rights while being able to detect and bypass the security systems elements. The operations engineer breaches the hardware security and uses standalone utilities to access files and log on to the system. Workstations are the network's most accessible components and are where most attempts at unauthorised action can be made. Workstations control information processing, run programs, enter and edit data, and the workstations disks can contain important data and processing programs. Servers need special protection. Some are hubs for large amounts of information, others are elements in which data transformation takes place while coordinating exchange protocols in different network sections. Here attackers will look for opportunities to affect the various subsystems work, using the delimiting remote access exchange protocols and means shortcomings to resources and system tables. All possibilities and means, up to special software tabs, are used to overcome the protection system. Communication channels and means pass through uncontrolled territory by communication lines length virtue and it is almost always possible to connect to them or interfere with the data transmission process by using malefactors. During information processing, possible origins, integrity violations, information veracity and integrity are

23 P.A. Deverka, M.A. Majumder, A.G. Villanueva, M. Anderson, A.C. Bekker, and J. Bardill. "Creating a data resource: What will it take to build a medical information commons?". *Genome Medicine* (2017), 9(84): 1-5.

24 K.A. Vinogradov and M.I. Nikitina. "Regional health information system formation". *Doctor and Information Technologies* (2014), 2: 10-12.

25 K.M. Smirnova. "The information security problem in the using the Things Internet context in medicine". *Medical Law* (2019), 1: 31-37.

committed by accidental or deliberately incorrect (unauthorised) user actions (authorised or unauthorised for operation in information protection systems)[26].

There are other hazards and channels for information leakage. These include the degree of information protection from unauthorised access and unlawful, which depends on the organisational and technical measures development quality aimed at excluding access to information processing equipment, controlling the various information carrier's removal by personnel, prohibiting unauthorised data entry or destruction. Information processing systems and illegal use of obtained data, access to information processing systems with improvised devices shall be prevented. Unauthorised data transmission via communication channels from the institution is prohibited. Data processing on-demand without the customer relevant requirement and the unauthorised reading, alteration or data destruction during transmission or data carriers' transportation is not permitted[27]. A secure health information system establishment requires establishment of a protection system, which is a regular process carried out at the health information protection systems lifecycle at all stages[28].

Different countries have different policies and laws for data privacy. For example, in Brazil, the public health system was established in 1988 by the Federal Constitution and is now known as the Sistema Único de Saúde (Unified Health System), better known by the acronym SUS. In Brazil, the main databases storing health-related information are generated from SUS. These databases can be classified into (1) epidemiological (such as the Live Births Information System/SINASC; the Mortality Information System/SIM; the Information System for Notifiable Diseases/SINAN), which are used for surveillance, evaluation, and research to address public health questions; (2) administrative (such as the Outpatient Information System/SIA-SUS and the Hospital Information System/SIH-SUS), which are used for accounting and control of the production of the services provided; and (3) clinical, which are used to store clinical data on patients for future reference[29]. In 2016, about

26 V.S. Kolomoytsev and V.A. Bogatyrev. "Multilevel protected access structural organization choice effectiveness and justification Estimation to external network resources". *Information and Space* (2015), 3: 71-79.

27 V.A. Bogatyrev. "To functional resources distribution in fault-tolerant multimachine computer systems". *Devices and Systems. Management, Control, Diagnostics* (2001), 12: 1-5.

28 A.A. Sogiainen. "Handling information constituting medical secrecy peculiarities". *Law in Armed Forces* (2017), 3: 26-31.

29 A.M.D.F.M. Souza, S.B. de Oliveira and E.P. Daher. "Mapping the hospital billing process: The case of a federal hospital in Rio de Janeiro". *Procedia Computer Science* (2016), 100: 671-676.

76% of major medical units used paper patient history. Due to this, there has been a need to computerise patient data management processes and several tools have been developed for this. One such tool is the electronic patient record (EHR)[30]. Until the end of 2019, legal regulations from professional associations restricted medical teleconsultations by phone or video conference in Brazil. When the COVID-19 pandemic began in 2020, teleconsultations provided the means to support access to quality health care to attend an in-person appointment. Legislation was introduced to allow teleconsultation, and several individual initiatives were quickly developed[31]. In Brazil, the protection of information is controlled by the Constitution, according to which the intimacy, private life, honour and image of the people are inviolable, with the assured right to indenisation by material or moral damage resulting from its violation[32].

Several stages can therefore be distinguished in the development of protection systems in medical information systems: the health care information system identifying the information and technical resources and facilities to be protected; identification of potential threats and information leakage channels'; information protection system resources carrying out vulnerability and risk assessment in the presence of multiple threats and leakage channels; determination of information protection system requirements; protection means and their characteristics; selection implementation; protection measures, methods and means use implementation and organisation; protection system integrity control and management implementation[33].

Specific features to ensure security and privacy in medical informatics are: completeness of initial information and certainty about the information systems composition and the threat; multi-criteria task to take into account the large number of information protection system indicators (requirements); both quantitative and qualitative indicators presence, which must be considered when

30 T. de Oliveira Vargas Yamada and F. Nascimento Almeida. *Perspectives of blockchain in digital health in Brazil.* (Cham: Springer, 2022).

31 S. de Camargo Catapan, A. Taylor and M.C.M. Calvo. "Health professionals' views of medical teleconsultation uptake in the Brazilian Unified Health System: A description using the NASSS framework". *International Journal of Medical Informatics* (2022), 168: 104867.

32 K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi and M. Saadi. "Big data security and privacy in healthcare: A review". *Procedia Computer Science* (2017), 113: 73-80.

33 S.I. Pospelova, Y.D. Sergeev, Y.V. Pavlova and N.A. Kamenskaya. "The legal regime for the use of telemedicine technologies and the introduction of electronic document management: The current state of legal regulation and development prospects". *Medical Law* (2018), 5: 24-33.

addressing the information protection systems design and implementation; the ability to implement methods for creating the projected protection system a model, allowing the requirements, indicators formation and evaluating the technical and organisational development of measures' effectiveness[34].

Conclusions

Having analysed the decision-making features of security and confidentiality in medical informatics, we can conclude that security system creation is an important, complex, knowledge-intensive task, which should be implemented by specialists in the information security field. In addition, such decisions adoption will contribute to improving the treatment and diagnostic process clinical effectiveness after a comprehensive patient safety system introduction – directly correlating with a decrease in the medical interventions complications number, long-term hospitalizations and unplanned rehospitalizations, transfers to other departments due to interventions complications, the nosocomial infection incidence. Also, security and confidentiality in medical informatics is of particular importance in the legal plane, since regulatory consolidation as a legal category makes this security and confidentiality fundamental for the legal support system. The medical information security and logical content certainty depends on scientific knowledge development, as well as on the public administration mechanism development. Medical information security understanding as a legal category should be based on its complexity understanding as a social phenomenon, and also take into account human information rights and freedoms as a meaningful content that determines this category essence.

The study results in this article are of both scientific-theoretical and practical interest, have been used and can be further used in:

– research purposes as a basis for the legal foundations of information security and confidentiality, further development in the health system in general, and the individual in particular; as well as for the theoretical and legal and methodological issues further development and its legal framework;

34 N.Z. Janjua, M. Kuo, M. Chong, A. Yu, M. Alvarez, and D. Cook. "Assessing Hepatitis C Burden and Treatment Effectiveness through the British Columbia Hepatitis Testers Cohort (BC-HTC): Design and characteristics of linked and unlinked participants". *Plos One* (2016), 11(3): e0150176.

- in law-making and law-enforcement activities to improve information and health care legislation processes; as a methodological basis for the relevant normative legal acts drafts scientific and legal expertise; as well as for improving security and confidentiality bodies activity in medical informatics;
- in the educational process in the preparation of teaching materials for relevant academic disciplines;
- in educational and outreach activities to improve citizens' legal and informational culture, their informational rights and freedoms awareness, and to identify and neutralise threats to information security in medical informatics.