European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 287-297
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 23

Health and Cybercrime*

Francesco Saverio Romolo
(Associate Tenured Professor of Legal Medicine at University of Bergamo)

Simone Grassi
(Type B University Researcher in Legal Medicine at University of Florence)

Alessandro Di Luca
(Medical Legal Expert at Coordinamento Generale Medico Legale of INPS)

Michela Previtali
(Degree in Law at University of Bergamo)

Antonio Oliva
(Full Professor of Legal Medicine at Università Cattolica del Sacro Cuore-Fondazione Policlinico Universitario A. Gemelli IRCCS, Rome)

ABSTRACT The importance of confidentiality in the practice of medical profession was recognised as a priority since the Hippocratic Oath. Internet caused a revolution not only in everyday life of citizens but also in the handling of health information by medical professionals. Exchange of health data can guarantee a better answer to the population health needs but also poses new risks. The European Union Agency for Network and Information Security (ENISA) published its first analysis of the cyber threat landscape of the health sector in the EU in July 2023.

Hospitals faced many different cyberattacks in the last years, sometimes with important economic consequences. This article reports the main classes of possible attacks, such as phishing, ransomware, data loss or data theft, attacks to connected medical devices, and Distributed-Denial-of-Service (DDoS), and the specific targets attractive for cybercriminals in the health information technologies (HIT), such as the electronic health records (EHR), the personal health records (PHR), the booking system for clinical appointments and the administrative systems. From a medico-legal perspective, it is paramount to frame in a correct manner the issue regarding current cybercrimes targeting healthcare structures.

The issue is well known for Patient Safety operators as a serious threat: a delay on data availability or the impossibility to obtain certain information in critical occasion could led to serious (if not fatal) consequences for the patient.

After examining the laws involved in protecting patients and their data from cyberattwacks, we conclude that addressing these threats cannot be solely based on legal means, but also IT and risk management strategies, together with the compliance with standards such as ISO 31000 are needed for a fruitful approach with a specific focus on digital expertise of healthcare professionals as well as administrative staff involved in healthcare.

1. *Health data*

1.1. *Historical introduction: from the Hippocratic Oath to the European Charter of Medical Ethics*

Confidentiality in the practice of medical profession is recognised as a priority since the time when the Hippocratic Oath was written.[1] The Hippocratic Oath demands physician to respect confidentiality: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about".[2]

In 1949 the World Medical Association published the first International Code of Medical Ethics (ICoME).[3]

The comparative studies of health legislation in Europe[4] prepared ground for the WHO Declaration on the Promotion of Patients' Rights in Europe, drafted in 1994, including the definition of the concept of medical secrecy: "4.1 All information about

[*] Article submitted to double-blind peer review.

[1] D.C. Smith, *The Hippocratic Oath and Modern Medicine*, in *Journal of the History of Medicine and Allied Sciences*, vol. 51, issue 4, 1996, 484–500.

[2] S.A. Antoniou, G.A. Antoniou, F.A. Granderath *et al.*, *Reflections of the Hippocratic Oath in Modern Medicine*, in *World J. Surg*., vol. 34, 2010, 3075–3079.

[3] World Medical Association published, *International Code of Medical Ethics*, available online at www.wma.net/policies-post/wma-international-code-of-medical-ethics.

[4] J.J. Leenen, G. Pinet and A.V. Prims, *Trends in health legislation in Europe*, WHO 1986.

patient's health status, medical condition, diagnosis, prognosis and treatment and all other information of a personal kind must be kept confidential, even after death. 4.2 Confidential information can only be disclosed if the patient gives explicit consent or if the law expressly provides for this. Consent may be presumed where disclosure is to other health care providers involved in the patient's treatment. 4.3 All identifiable patient data must be protected. The protection of data must be appropriate to the manner of their storage. Human substances from which identifiable data can be derived must be likewise protected".[5]

Internet caused a revolution in everyday life including the handling of health data. Their exchange among healthcare professional can guarantee a better answer to the requests of health from patients but also poses new risks of mishandling of information related to the health condition of people.

On 10 June 2011 the European Charter of Medical Ethics was adopted.[6] According to its Principle 5 "The physician is the patient's essential confidant. He betrays this confidence on revealing what he has learned from the patient". Based on this principle, Deontological Guidelines were established by the European Council of Medical Orders (ECMO), stating about professional secrecy: "The physician must ensure the patient absolute secrecy on all the information he has collected. Confidentiality covers everything that physicians have learned in the exercise of their profession, that is to say not only what they were told in trust, but also what they may have observed, heard or understood. Medical confidentiality is not abolished by the death of patients. The physician informs people assisting him about their obligations as regards secrecy, asking, whenever possible to give a written undertaking. Derogations, when they exist, are strictly provided for in national legislations".

The importance of the subject pushed the establishment of the Task Force on Privacy and the Protection of Health-Related Data in 2017 by the UN Special Rapporteur on the right to privacy. Its aim was to prepare a recommendation on the protection and use of health-related data for Member States to use as an international baseline of minimum data protection standards for health-related data.[7]

1.2. *Personal data in Europe*

The article 8 of the Charter of fundamental rights of the European Union is about the "Protection of personal data" and states that: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".[8]

The need to reduce or avoiding the risks connected to wrongful processing of data resulted in the Data Protection Directive in 1995.[9] On 25 January 2012 the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules[10] and in 2016 the EU adopted the General Data Protection Regulation (GDPR), applicable as of 25 May 2018 in all member states.[11]

According to GDPR, anyone who decides 'why' and 'how' personal data are processed is a data controller. Among the tasks the data controller must fulfil is the implementation of appropriate technical and organisational

[5] M.E. Sokalska, *Medical Confidentiality – Quo Vadis?*, in *European Journal of Health Law*, vol. 11, issue 1, 2004, 35-43.

[6] *European Charter of Medical Ethics*, 2011, available online at www.ceom-ecmo.eu/sites/default/files/documents/en-european_medical_ethics_charter-adopted_in_kos.pdf.

[7] UN Special Rapporteur on the right to privacy, *Report on the Protection and Use of Health-Related Data*, 2019.

[8] European Union: Council of the European Union, *Charter of Fundamental Rights of the European Union* (2007/C 303/01), 14 December 2007, C 303/1, available at: www.europarl.europa.eu/charter/pdf/text_en.pdf.

[9] European Union. Directive (EC) 95/46 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 [1995] OJ L281/31 ('Directive 95/46/EC').

[10] V. Reding, *The European data protection framework for the twenty-first century*, in *International Data Privacy Law*, vol. 2, No. 3, 2012, 119-129.

[11] European Union, Regulation 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation), which was approved and come into force on 27 April 2016, (2016) available at https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679 last access on 12 July 2023.

protection measures against data breach. A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A possible approach to protect personal data is to render them unintelligible to any person who is not authorised to access it (encryption).

In recent years, physicians and patients have been extensively using computerized technologies and digital information. Data related to health are collected by physicians and shared through network systems. The central ethical issue stemming from the use of electronic records is the need for an equilibrium between the right to health and the risk of leaking confidential medical information.

The GDPR defines 'data concerning health' as personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. This definition is an extensive one because it regards even the data that can reveal the health status or risk of patient only if combined with other information[12]. Health data can be processed if the patient, called "data subject", has given consent to their processing for one or more specific purposes.

The main reason to collect health data is to support the delivery of healthcare (this use is known as the "primary use of data").[13] The recent COVID-19 outbreak clearly demonstrated how access to health data is also important for scientific research and policy-making purposes (known as the "secondary use of data").[14] [15] According to GDPR, the explicit consent of the data subject can be waived, for example, for reasons of substantial public interest or for scientific research.[16]

The EU Commission published in May 2022 a proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (EHDS), seeking to ensure the people's control over their health data, allow harmonised and interoperable electronic health record (EHR) systems across the EU and build a framework for the secondary use of health data for research, innovation and policymaking to improve population's health.[17]

The right to the protection of health data is not an absolute right anymore, protected by professional secrecy; it must be considered nowadays "in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality".[18]

The massive quantities of health data collected over the last decades resulted in growing enthusiasm for the potential usefulness of these in transforming personal care, clinical care and public health.[19]

The use of Big Data in healthcare poses not only new ethical and legal challenges because of the personal nature of the information involved but also new technical and organisational challenges related to the need of allowing effective exchange and use of health data while protecting them by attacks aiming to possible illegal use (e.g. data breaches).[20]

2. *Cybercrime targeting the healthcare system*

According to EU Cybersecurity Act, a cyber threat is "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such

[12] V. Hordern, *Data protection compliance in the age of digital health*, in *Eur. J. Health Law*, vol. 23, 2016, 248-264.

[13] R. Hussein, L. Scherdel, F. Nicolet and F. Martin-Sanchez, *Towards the European Health Data Space (EHDS) ecosystem: A survey research on future health data scenarios*, in *Journal of Medical Informatics*, vol. 170, 2023, 104949.

[14] C.J. Wang and R.H. Brook, *Response to COVID-19 in Taiwan: big data analytics, new technology, and proactive testing*, in *JAMA*, vol. 323, 2020, 1341-1342.

[15] C. Cosgriff, D. Ebner and L. Celi, *Data sharing in the era of COVID-19,* in *Lancet Digit Health*, 2020, no. 2224.

[16] A. Oliva, S. Grassi, G. Vetrugno, R. Rossi, G. Della Morte, V. Pinchi and M. Caputo, *Management of Medico-Legal Risks,* in *Digital Health Era: A Scoping Review*, in *Front. Med.*, vol. 8, 2022, 821756.

[17] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197, 2022.

[18] European Union, General data protection regulation, Off J Eur Union 49 (2016) L119 available online at https://gdpr-info.eu.

[19] E. Vayena, J. Dzenowagis, J.S. Brownstein and A. Sheikh, *Policy implications of big data in the health sector*, in *Bull World Health Organ*, 2018, no. 96, 66–8.

[20] R. Pastorino, C. De Vito, G. Migliara, K. Glocker, I. Binenbaum, W. Ricciardi and S. Boccia, *Benefits and challenges of Big Data in healthcare: an overview of the European initiatives*, in *European Journal of Public Health*, vol. 29, 2019, issue supplement 3, 23–27.

systems and other persons”.[21] The Cybersecurity Act followed the Directive 2016/11481 on security of network and information systems (the NIS Directive), which was the first EU legislation for the protection of network and information systems across the Union.[22] The trust in digital technologies is especially needed in many sectors which are vital for the society, including healthcare, which are suffering deliberate attacks to their network and information systems by criminals in recent times. Any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT) can be defined as cyber-dependent crime. An example is the creation and spread of malware, but criminals also hack to steal sensitive personal or industry data or attacks to cause denial of service, resulting in financial and/or reputational damage.[23]

Malwares are the most frequent sort of computer, network, or user attacks to cause damage or steal sensitive information.[24] Healthcare facilities must now deal not only with malwares but with many different cyber risks, i.e. “operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems”.[25]

The European Union Agency for Network and Information Security (ENISA) was founded in 2004 as the specialised EU agency. ENISA published its first analysis of the cyber threat landscape of the health sector in the EU, reporting cyber incidents from January 2021 to March 2023 in the health sector in July 2023.[26]

2.1. *A little history about health and cybercrime*

It is interesting that the first ransomware attack had a healthcare theme. In 1989 Joseph Popp, an AIDS researcher, distributed thousands of ‘floppy disks’ to other AIDS researchers, spreading a malware across more than 90 countries. The software locked the computer and showed on the screen the request for a payment when the system was powered on 90 times.[27]

In the following years hospitals were attacked in many different ways, sometimes with important economic consequences. An example occurred on 20 March 2014, when numerous hosts attacked the Boston Children’s Hospital, causing a network outage called Distributed Denial of Service (DDoS), adversely disrupting hospital operations for two weeks.[28]

In April 2014 attackers gained access to the database of Anthem, the second largest health insurance company in the USA.[29] The breach originated from an employee, who opened a phishing email, allowing the threat actor to gain access to the employee’s computer. The attack was first discovered on 27 January 2015 and affected not-encrypted personally identifiable information (PII) of almost 80 million customers, including records of at least 12 million minors, and alerted federal authorities.[30] In August 2018 the final

[21] European Union, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), available online at https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[22] D. Markopoulou, V. Papakonstantinou and P. de Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation*, in *Computer Law & Security Review*, vol. 35, 2019, issue 6, 105336.

[23] Europol, *Internet Organised Crime Threat Assessment 2018* (2019), available online at www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.

[24] F.A. Aboaoja, A. Zainal, F.A. Ghaleb, B.A.S. Al-rimy, T.A.E. Eisa and A.A.H. Elnour, *Malware Detection Issues, Challenges, and Future Directions: A Survey*, in *Applied Sciences*, 12, 2022, 1.

[25] A. Sardi, A. Rizzi, E. Sorano and A. Guerrieri, *Cyber Risk in Health Facilities: A Systematic Literature Review*, in *Sustainability*, vol. 12, 2020, 1. doi: https://doi.org/10.3390/su12177002.

[26] European Union Agency for Network and Information Security, *ENISA Threat Landscape: Health Sector*, available online at www.enisa.europa.eu/publications/health-threat-landscape.

[27] C. Mehra, AK. Sharma and A. Sharma, *Elucidating Ransomware Attacks in Cyber-Security*, in *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9, Issue 1, 2019, 3536-3541.

[28] *Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies*, available online at www.proquest.com/openview/c5af58f60f7c269ac04918fa2382f05e/1?pqorigsite=gscholar&cbl=544481.

[29] Y.Y. Leong and Y.C. Chen, *Cyber risk cost and management in IoT devices-linked health insurance*, in *Geneva Pap Risk Insur Issues Pract 45*, 2020, 737–759.

[30] L.H. Yeo and J. Banfield, *Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis*, in *Perspect. Health Inf Manag*, 2022 Mar 15; 19 (Spring) available online at www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/#B2

approval was given to a $115 million settlement that ended further claims against Anthem over its data breach.[31] In October 2020 a coalition made up of 44 states and Washington D.C. reached a $39.5 million settlement with Anthem, to resolve the claims stemming from the 2014 cyberattack.[32]

Another example is what happened on February 2016, when Hollywood Presbyterian Medical Center was attacked by a ransomware, disrupting the systems and making patient data unusable. It was the first attack that put human lives at risk (threatening to turn off life-saving equipment) and the Medical Center paid the 40 bitcoins ransom ($17,000 in 2016) to recover their files.[33]

A global ransomware attack, called WannaCry, struck about 200,000 systems across 150 countries on 12 May 2017. Only considering the British National Health Service (NHS), at least 80 out of 236 trusts across England were affected: 34 infected hospital trusts (NHS organisations that provide acute care, specialised medical services, mental healthcare, or ambulance services) were locked out of their digital systems and medical devices, such as Magnetic resonance imaging (MRI) scanners; 46 affected hospital trusts were not infected but reported disruption. Appointments cancelled identified by NHS England were 6,912, but calculations based on the normal rate of follow-up appointments to first appointments estimated more than 19,000 appointments cancelled.[34] Hospitals directly infected with the ransomware had 4% fewer emergency admissions and 9% fewer elective admissions were recorded the total economic value of the lower activity at the infected trusts during this time was £5.9 million.[35]

During the COVID-19 pandemic, unprecedented cybersecurity concerns related to emerged phishing attacks.[36] To give more details, a website very similar to the WHO'S internal email was developed by some hackers; the achievement they were looking for was to obtain credentials by stealing them from WHO workers.[37] [38]

In the Czech Republic on 12 March 2020 the Brno University Hospital had to close down its whole IT network. This developed consequences on different branches of the hospital such as the Children's Hospital and the Maternity Hospital.[39] It caused the necessity not only to delay urgent surgical interventions but also to redirect the new serious patients to a hospital close nearby. To retrieve the network, different groups collaborated to reach the goal, in particular teams from NCSC (the Czech National Cyber Security Centre), NCOZ (the Czech Police) and the IT staff from the hospital.[40]

Another example is what happened on 9 September 2020, when a ransomware hit the Düsseldorf University Hospital. Specifically, thirty servers were compromised, it was impossible to access patients' data and many of the medical equipment connected to the Wi-Fi were unavailable. In this confused

0.

[31] F. Donovan, *Judge Gives Final OK to $115M Anthem Data Breach Settlement*, in *Health IT Security*, 2018 available online at https://healthitsecurity.com/news/judge-gives-final-ok-to-115m-anthem-data-breach-settlement.

[32] J. Davis, *Anthem Settles with 44 States for $40M Over 2014 Breach of 78.8M*, in *HealthITSecurity*, 2020, available online at https://healthitsecurity.com/news/anthem-settles-with-44-states-for-40m-over-2014-breach78.8m?_cf_chl_tk=m1v9sXfqVLFDH4kcos62u_pecIqSFwpwVSvQmhjfz_I-1690222749-0-gaNycGzNDPs.

[33] T. Hofmann, *How organisations can ethically negotiate ransomware payments*, in *Network Security*, issue 10, 2020, 13-17, available online at https://digpath.co.uk/wpcontent/uploads/2020/10/NESE_2020-10_Oct.pdf.

[34] National Audit Office, *Investigation: WannaCry cyber-attack and the NHS*, 2017, available online at www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[35] Ghafur, S., Kristensen, S., Honeyford, K. *et al*, *A retrospective impact analysis of the WannaCry cyberattack on the NHS*, in *Npj Digit. Med*, 2, 2019, 98, available online at www.nature.com/articles/s41746-019-0161-6#citeas.

[36] N. O'Brien, S. Ghafur, A. Sivaramakrishnan and M. Durkin, *Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that*, in *Digital Health*, vol. 8, 2022, 1-3.

[37] B. Kale, S. Aworo and C. Anyangwu, *Cyber-Attacks on Digital Infrastructures in HealthCare: The Secured Approach*, 2022, 1-12, available online at www.researchgate.net/publication/366323639.

[38] A.F. Al-Qahtani and S. Cresci, *The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19*, in *IET Inf Secur*, vol. 16, issue 5, 2022, 324-345.

[39] F. Gioulekas, E. Stamatiadis, A. Tzikas, K. Gournaris, A. Georgiadou, A. Michalitsi-Psarrou, G. Doukas, M. Kontoulis, Y. Nikoloudakis, S. Marin, R. Cabecinha and C. Ntanos, *A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures*, in *Healthcare*, vol. 10, issue 2, 2022, 1-19.

[40] S. Parker and C. Mancarella, *Trust-IT, PANACEA Healthcare Cybersecuirity Advisory Services, COVID-19 is extending the cyber threat surface as healthcare organisations come under increasing strain*, 2020, available online at: www.panacearesearch.eu/watch/blog/covid-19-extending-cyber-threat-surface-healthcare-organisations-comeunder-increasing.

scenario there was a 78-year-old patient who was, due to a brain aneurysm, waiting for an emergency operation. The patient unfortunately died after the delay due to redirecting the ambulance to the Wuppertal Hospital.[41] [42]

Also, it is reported the first closure of an hospital related to a ransomware attack: the Saint Margaret's Health in the USA, occurred on 16 June 2023. The attack happened in 2021 and prevented the presentation of compensation's requests for months. The reported average cost to recover from a ransomware attack in the USA was 4,35 milions dollars.[43]

Another example is the Irish health system's IT infrastructure, which suffered a ransomware attack in May 2021. It impacted more than 80% of the system causing data theft and a hindrance to healthcare workers, who could not enter non clinical systems (such as finance and procurement) and clinical systems in order to give patients the required care. It took four months for the service to fully recover.

On August 2022, the Center Hospitalier Sud Francilien situated in Paris was hit by a ransomware attack and to obtain the decription key, the Center was required to pay $10,000,000.[44]

In 2022 Costa Rica suffered major ransomware attacks and for the first time a country has declared a "national emergency" in response to a cyberattack. According to the Costa Rican Social Security Fund the attack targeting Costa Rica's health care system at the end of May affected 484,215 medical appointments, needing massive rescheduling.[45]

The reported cases are only a selection of possible attacks, which can be grouped in the following classes.

1. Phishing by email;
2. Ransomware, which is "a malware that works by encrypting data saved in computers or the network itself. A ransomware attack is a malicious software that eliminates access to user data by encrypting" can be "cryptor" or "blocker". There are also "ransomware as a service (RaaS)", allowing to make a cyberattack to people without any specific knowledge.
3. Data loss or data theft.
4. Attacks to connected medical devices, considering that a medical device is defined as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or another similar or related article, including a part or accessory, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease".
5. Distributed-Denial-of-Service (DDoS).[46]

In the "2021 HIMSS Healthcare Cybersecurity Survey", "phishing" and "ransomware" are reported as the most frequent attacks.

According to the latest report by Europol, the cyber-attacks based on malwares are still the most prominent threat, with ransomware maintaining its position of the top threat. After the Russian attack against Ukraine, Distributed Denial of Service (DDoS) attacks against EU targets significantly increased.[47]

3. *Risks for patients in health structures*

Several factors make health care organizations attractive to would-be hackers, one being the economic value of data in the "*dark web*".[48]

Specific targets in the health information technologies (HIT) are:
- the electronic health records (EHR);
- the personal health records (PHR);
- the booking system for clinical appointments;
- the administrative system.

These targets are attractive for

[41] R. Shandler and M. A. Gomez, *The hidden threat of cyber-attacks – undermining public confidence in government*, in *Journal of Information Technology & Politics*, vol. 20, Issue 4, 2023, 359-374.

[42] A. Sunil Lekshmi, *Growing Concern on Healthcare Cyberattacks & Need for Cybersecurity*, 2022, 1-4.

[43] R. Patano, *Ransomware, le tecnologie avanzate per limitare i danni*, 2023. Available online at: www.agendadigitale.eu/sicurezza/ransomware-ecco-le-tecnologie-avanzate-per-limitare-i-danni.

[44] M. Horduna, S.-M. Lăzărescu and E. Simion, *A note on machine learning applied in ransomware detection*, in *Cryptology ePrint Archive*, 2023, 1-17.

[45] M. Burgess, *Conti's Attack Against Costa Rica Sparks a New Ransomware Era*, WIRED, 2022, available online at: www.wired.com/story/costa-rica-ransomware-conti.

[46] M.A. Ahmed, H.F. Sindi and M. Nour, *Cybersecurity in Hospitals: An Evaluation Model*, in *Cybersecurity and Privacy*, vol. 2, 2022, 854-855.

[47] Europol, *Europol Spotlight - Cyber-Attacks: The Apex Of Crime-as-a-Service*, 2023, available online at www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf.

[48] S.T. Argaw *et al.*, *The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review*, *op. cit.*, 2.

cybercriminals: Personal Health Information (PHI) is bought and sold on the dark web for more than 10 times the amount of stolen credit card information, making it the most expensive data on the criminal market. The value is derived from the data points in the record that, when combined, can be used to create fake IDs, to buy medical equipment, write prescriptions and file false insurance claims. The multiple relationships, multiple touchpoint and multiple facilities of the industry make it susceptible to a variety of attacks. For example, a typical patient experience for an outpatient surgery can involve an initial encounter at the physician's office, an eligibility check with the insurance company, office contact to schedule the procedure, admission to the centre for surgery, and a pharmacy visit to have prescriptions filled.

The increased use of the "internet of medical things" devices, such as patient monitoring devices, which collect data, exchange data and are connected to the outside world, provides a major opportunity for security breaches. In addition, patients' growing demand for instant access to their data, combined with online scheduling capability, further exacerbates the challenge of ensuring the security of health care organizations' data systems.

From a medico-legal perspective, it is paramount to frame in a correct manner the issue regarding current cybercrimes targeting healthcare structures. If cybersecurity on one had is typically administered as a corporate tool for risk management as in for every enterprise in and beyond healthcare, in our digital era the access (or lack of) to data and the correct functioning of medical devices has become a major issue in administering Patient Safety. The issue is well known[49] [50] as a serious concern for Patient Safety operators.

One of the primary concerns in cybercrime prevention is the risk of unauthorized access to patient data. If healthcare systems are not properly secured, malicious individuals could gain unauthorized access to sensitive information such as medical history, diagnoses, treatment plans, and personal identifiers. This can lead to identity theft, fraud, or misuse of the data. Healthcare organizations store vast amounts of valuable data, making them attractive targets for cybercriminals. Data breaches can occur due to security vulnerabilities, human error, or sophisticated hacking techniques. When a breach happens, it can result in the exposure of sensitive patient information, leading to privacy violations and potential harm to patients.[51] [52] Data loss can occur due to hardware failures, software glitches, natural disasters, or cyberattacks. Inadequate backup systems or improper data management practices can lead to permanent loss of critical patient data, potentially impacting patient safety and continuity of care. It is also crucial to keep in mind that healthcare data is crucial for providing quality care and making informed medical decisions and that a delay on data availability or the impossibility to obtain certain information in critical occasion could led to serious (if not fatal) consequences for the patient. Ensuring secure data exchange and maintaining patient privacy during data sharing processes are critical challenges. In an interconnected healthcare ecosystem, sharing patient data across different systems and organizations is essential for coordinated care.[53] However, this also introduces potential vulnerabilities that require robust encryption methods, data access controls, and compliance with relevant regulations, especially considering that healthcare employees, contractors, or business associates with authorized access to patient data can also pose a security risk that may involve unauthorized use, disclosure, or modification of sensitive information for personal gain, revenge, or negligence.[54]

[49] L. Coventry and D. Branley, *Cybersecurity in healthcare: A narrative review of trends, threats and ways forward*, in *Maturitas*, vol. 113, 2018, 48-52. doi: 10.1016/j.maturitas.2018.04.008. Epub 2018 Apr 22. PMID: 29903648.

[50] C.S. Kruse, B. Frederick, T. Jacobson and D.K. Monticone, *Cybersecurity in healthcare: A systematic review of modern threats and trends*, in *Technol. Health Care*, vol. 25, issue 1, 2017, 1-10.

[51] A.H. Seh, M. Zarour, M. Alenezi, A.K. Sarkar, A. Agrawal, R. Kumar and R.A. Khan, *Healthcare Data Breaches: Insights and Implications*, in *Healthcare (Basel)*, vol. 8, no. 2, 13 May 2020, 133.

[52] A. Almalawi, A.I. Khan, F. Alsolami, Y.B. Abushark and A.S. Alfakeeh. *Managing Security of Healthcare Data for a Modern Healthcare System*, in *Sensors (Basel)*, vol. 23, no. 7, 30 Mar 2023, 3612.

[53] S. Canali, V. Schiaffonati and A. Aliverti, *Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness*, in *PLOS Digit Health*, 13 Oct 2022, vol. 1, no. e0000104.

[54] L.T. Martin, C. Nelson, D. Yeung, J.D. Acosta, N. Qureshi, T. Blagg, and A. Chandra, *The Issues of Interoperability and Data Connectedness for Public*

e-Health: New Frontiers and Challenges for Healthcare

For all the aforementioned reasons healthcare data protection is subject to various legal and regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. Compliance with these regulations involves implementing technical and organizational measures to safeguard patient data, conducting risk assessments, and ensuring proper consent and authorization procedures. Addressing these concerns requires a multi-faceted approach, including implementing cybersecurity measures, conducting regular risk assessments, training staff on data protection protocols, establishing strong access controls, encrypting sensitive data, and ensuring regulatory compliance.[55]

Data protection is, therefore, a core duty of any health institution, to allow the appropriate cure of patients and to avoid secondary use of health information, which may expose the patient to legal (e.g., identity theft), economic or social (e.g., discrimination in health insurance or employment) negative consequences. Moreover, even when none is harmed by a data breach, there could still be deontological concerns.[56] The two major risks are represented by breach of confidentiality and breach of security. In the first case, the healthcare professional who received the personal information by the patient unlawfully discloses it to third parties. This scenario occurs not only when the information is transmitted without patient's consent, but more generally when there is no legal obligation to disclose confidential information. In this case, regulations and legal sanctions could be considered per se a proper response, being able to offset the risk. Instead, breach of security entails unauthorized access and/or use of personal information by people who were not involved in the physician-patient relationship. While the security of data generated by health care system, like those contained in health records, is heavily regulated, health-relevant data obtained through medical devices are generally considered to be more exposed to the risk of security breaches, especially in some countries.[57] Indeed, the regulatory frameworks largely vary among different countries, with European Union regulations generally considered broader than US sector-specific laws.[58] However, compliance with regulations (e.g., anonymization of data) does not mean to eradicate the risks for patients' privacy. For instance, GDPR and California Consumer Privacy Act require stringent criteria for data deidentification (since deidentified data are substantially no subject to regulation), but artificial intelligence can be able to reidentify information.[59] Therefore, health institutions must manage these risks implementing data security and access control measures.[60]

First, health institutions must limit data collection, ensure the minimalization, and must be always able to prove the equitability of the process (in order to contain specific risks, like that of biases).

Moreover, the data lifecycle must be clearly set and described, analyzing the risks of data leakage specific for any phase. That being said, access remains a crucial part of the process, being critical for both the user and the institution. Indeed, access to health services, including artificial intelligence products and wearables producing/storing/using sensitive data, is a core indicator of performance for health care systems.[61] Direct access to medical information is a legal right with a critical impact on patients' satisfaction, ability to recall and understand medical information,

Health, in *Big Data*, vol. 10, S1, 2022, S19-S24.

[55] E. Negro-Calduch, N. Azzopardi-Muscat, R.S. Krishnamurthy and D. Novillo-Ortiz, *Technological progress in electronic health record system optimization: Systematic review of systematic literature reviews*, in *Int J Med Inform*, vol. 152, 2021, 104507.

[56] W.N. Prince 2nd and I.G. Cohen, *Privacy in the age of medical big data*, in *Nature Medicine*, vol. 25, issue 1, 2019, 37-43.

[57] D. McGraw and K.D. Mandl, *Privacy protections to encourage use of health-relevant digital data in a learning health system*, in *NPJ Digital Medicine*, vol. 4, 2021, Article number: 2.

[58] D. Grande, X. Luna Marti, R. Feuerstein-Simon, R.M. Merchant, D.A. Asch, A. Lewson and C.C. Cannuscio, *Health Policy and Privacy Challenges Associated With Digital Technology*, in *JAMA Network Open*, vol. 3, issue 7, 2020, e208285.

[59] B. Murdoch, *Privacy and artificial intelligence: challenges for protecting health information in a new era*, in *BMC Medical Ethics*, vol. 22, 2021, Article number: 122.

[60] K. Abouelmehdi, A. Beni-Hessane and H. Khaloufi, *Big healthcare data: preserving security and privacy*, in *Journal of Big Data*, vol. 5, issue 1, 2018, 1-8.

[61] J.F. Levesque, M.F. Harris and G. Russell, *Patient-centred access to health care: conceptualising access at the interface of health systems and populations*, in *International Journal for Equity in Health*, vol. 12, 2013, 1-9.

autonomy, and self-efficacy.[62] [63] Moreover, it is proven to increase organizational efficiency in health care facilities, also in particularly complex entities like mental institutions.[64]

Digital access is generally preferred by both healthcare professionals and patients, especially those facing barriers to healthcare access.[65] [66] Hence, specific policies must be implemented to address the risk of unauthorized digital access to information, designing safe authentication processes, encrypting/masking sensitive data to avoid unauthorized accesses, and governing accesses in compliance with an access control policy specifying privileges and rights of each authorized user (e.g., creating health data access level categories based on the trustworthiness of the user).[67] Finally, fostering effective patients-institution communication (aimed at increasing the transparency of the processes) and education of the healthcare professionals, who should be aware that the use even of deidentified data is never a zero-risk operation, are key interventions.

Regarding the risks, they are not limited to "internal failures" (e.g., unauthorized access to digital infrastructure of the institution) but also to external attacks, like ransomware attacks.[68]

The examples reported in this article show how ransomware attacks expose a significantly higher share of patients to the threat of data breach and can have catastrophic implications also in terms of patient safety (e.g., external control over medical devices/inhibited care due to disruptions), reputational damages and compensations/penalties caused by direct damages and failure to meet regulations.[69] In these cases, root cause analysis is often jeopardized by poor quality/quantity of data regarding attacks: indeed, hospitals usually are not compelled to report all the operational disruptions and they fail to do so especially when the event did not cause a direct harm for the patient. Addressing this threat in a multidisciplinary way (combining technical and medical expertise) should be seen as a public health priority, since cyber threats can jeopardize entire healthcare networks, propagating or even through the sole subsequent operational downtimes.[70] Ignoring the exact frequency and sophistication of the phenomenon exposes healthcare institutions and decision-makers to the risk of developing inappropriate responses or failing to develop responses to this growing issue. On the other side, an exact awareness of the issue means enabling decision-makers to tailor technical interventions and empowering safety culture among healthcare personnel.

In general, the spectrum of potential vulnerabilities and then the spectrum of potential interventions are broad. The main cause of events is represented by the human error (e.g., opening a phishing email), whose likelihood in turn can be boosted by preventable organizational factors such as excessive workload and reduced in case of proper training. Low awareness of cyber risks and of their implications is also another critical factor, also because it entails other risk factors like poor budgeting. Moreover, some radical changes (enhanced by the COVID-19 pandemic) in the work routine can influence

[62] S.E. Ross and C.T. Lin, *The effects of promoting patient access to medical records: a review*, in *Journal of the American Medical Informatics Association*, vol. 10, issue 2, 2003, 129-138.

[63] B. Fisher, V. Bhavnani and M. Winfield, *How patients use access to their full health records: a qualitative study of patients in general practice*, in *Journal of the Royal Society of Medicine*, vol. 102, issue 12, 2009, 539-544.

[64] A. Tapuria, T. Porat, D. Kalra, G. Dsouza, S. Xiaohui, and V. Curcin, Im*pact of patient access to their electronic health record: systematic review*, in *Informatics for Health and Social Care*, vol. 46, issue 2, 2021, 194-206.

[65] A. Scantlebury, A. Booth and B. Hanley, *Experiences, practices and barriers to accessing health information: A qualitative study*, in *International Journal of Medical Informatics*, vol. 103, 2017, 103-108.

[66] N. Bhandari, Y. Shi and K. Jung, *Seeking health information online: does limited healthcare access matter?*, in *Journal of the American Medical Informatics Association*, vol. 21, issue 6, 2014, 1113-1117.

[67] D. Xiang and W. Cai, *Privacy Protection and Secondary Use of Health Data: Strategies and Methods*, in *BioMed Research International*, vol. 2021, 2021, Article ID 6967166.

[68] H.T. Neprash, C.C. McGlave, D.A. Cross, B.A. Virnig, M.A. Puskarich, J.D. Huling, A.Z. Rozenshtein and S.S. Nikpay, *Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations*, in *2016-2021 JAMA Health Forum*, vol. 3, issue 12, 2022, e224873-e224873.

[69] M. Evans, Y. He, L. Maglaras and H. Janicke, *HEART-IS: A novel technique for evaluating human error-related information security incidents*, in *Computers & Security*, vol. 80, 2019, 74-89.

[70] C. Dameff, J. Tully, T.C. Chan, E.M. Castillo, S. Savage, P. Maysent, T.M. Hemmen, B.J. Clay and C.A. Longhurst, *Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments,* in *the US*, in *Jama Network Open*, vol. 6, issue 5, 2023, e2312270-e2312270.

the cyber risks: for instance, remote work (e.g., telemedicine) exposed the network to additional vulnerabilities, especially when unprotected wireless connections are used. Finally, inadequate protection of endpoint devices (e.g., laptops, medical devices) can represent an unprotected entry point for external attacks. As said, proper interventions require a combined and coordinated approach that includes IT resources and risk management experts. Indeed, besides technical interventions (e.g., secure remote work environment, regular software updates, creation of strong passwords, appropriate user authentication and data encryption), education (e.g., promotion of cyber culture) and management of human errors are crucial.[71] [72] Methods of human reliability analysis encompassing proper incident reporting and sharing processes have been recommended for dealing with human errors. For instance, Evans et al. proposed a combined mapping/analysis method (HEART-IS: Human Error Assessment and Reduction Technique of Information Security) to allow for root cause analysis and in particular to classify the human error (e.g., distinguishing omissive from commissive conducts), obtain descriptive information (e.g., role and frequency of the task that led to the error), and analyze all the error producing conditions (i.e., the conditions that could have increased the risks of error).

It is worth mentioning and underlining, once more, that the potential risks for patients due to cybercrime are not just damages related to privacy issues. The loss of data or the inoperability of a network or a medical device can lead directly (in medico-legal terms without the interruption of the causal link, meaning full liability on behalf of the Healthcare Enterprise) to a threat to the actual health of a patient and consequently biological damage (including certainly fatal events) that will require evaluation and compensation. The transposition of a digital risk to a very practical problem with physical consequences just mirrors our society's interdependence from digital devices and data, and ignoring such link represents a huge liability and vulnerability for every kind of healthcare structure. As in many other health-related areas concerning both risk management and patient safety, a more integrated approach would be preferable. A stricter collaboration with an approach that encompasses both cybersecurity and a more medico-legal perspective with an evaluation of threats and potential damages could lead towards a safer environment and a more conscientious use of digital data and devices from healthcare professionals.

The *"Healthcare Cybersecurity"* study by "*Bitdefender*", presented at the "*Healthcare Security Summit 2021 of Clusit*" pinpointed the following critical points:

- operating systems expired or not updated;
- inadequate protection of medical devices;
- no continuous control of risks of cyberattacks;
- too few specialists;
- inadequate funding compared to the threads.[73]

The situation will be more and more difficult to handle with the internet of medical things, allowing immediate data exchange. The development of the new resulting cyber ecosystems implies new cyber-risks.[74]

In Europe the situation is differentiated country by country in term of health systems. Italy, Finland and Sweden followed different path in national and regional policies about e-Health between 2009 and 2019.[75] Germany used resources from the Recovery and Resilience Plan for public health services, including digital infrastructure, telemedicine and information technology and cybersecurity.[76] A World Health Organization Europe project about health system transformation compared three European

[71] Y. He, A. Aliyu, M. Evans and C. Luo, *Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review*, in *Journal of Medical Internet Research*, vol. 23, issue 4, 2021, e21747.

[72] J.G. Ronquillo, J. Erik Winterholler, K. Cwikla, R. Szymanski and C. Levy, *Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information*, in *JAMIA Open*, vol. 1, issue 1, 2018, 15-19.

[73] Agenda Digitale, *Sanità italiana nel mirino del cyber-crime: grosso guaio per tutti i pazienti*, 2022, available online at www.agendadigitale.eu/sicurezza/sanita-nel-mirino-del-cyber-crime-cosi-litalia-rischia-grosso

[74] M.E. Watkins, D*esigning an Effective Organizational Culture to Guard Against the Cyber Risks of Emerging Technologies*, in *Journal of Healthcare Management*, vol. 68, issue 4, 2023, 239-250.

[75] H. Valokivi, S. Carlo, E. Kvist and M. Outila, *Digital ageing in Europe: a comparative analysis of Italian, Finnish and Swedish national policies on eHealth*, in *Ageing and Society*, vol. 43, issue 4, 2023, 835-856.

[76] European Commission, *State of Health in the EU: Synthesis Report 2023*, 2023, available online at https://health.ec.europa.eu/system/files/2023-12/state_2023_synthesis-report_en.pdf.

countries: Portugal, Sweden and UK. If on one hand in Portugal legislation is seen as an essential tool, on the other hand in Sweden and the UK legal means alone are considered insufficient for improving health systems.[77]

If the same legal approach cannot be followed neither all over Europe nor in a single country as Italy, where the health administration responsibility is shared between the central government and the different regions, approaches based on standards can be more appropriate.

A fruitful support to risk management is the ISO 31000 standard, published in 2009 and updated in 2018. It is a guideline for organizations that adopt a risk management model, based on fundamental principles. The first is an orientation towards continuous improvement. Others are to be dynamic and adaptable to evolving scenarios and enhance and build on the skills and knowledge of the human resources involved in functions and processes.[78] The model proposed by the ISO 31000 standard is based on risk assessment and risk treatment.[79] According to Ferdosi et al. risk evaluation in healthcare organizations must include the comparison of the results of the risk analysis with the risk evaluation criteria defined during the context establishment to determine whether the cyber-risks are acceptable.[80]

Healthcare sector is nowadays very concerned with clinical risks but cyber-risks are becoming more and more important not only because of the legal consequences due to the misuse of the data of patients but also because the cyber-attacks can prevent health organizations from treating their patients.

4. *Conclusion*

Health information storage and security have been revolutionized by information technologies for the last decades, going from handwritten notes to “immaterial” data stored in interconnected devices and/or in logical pools (“clouds”). This revolution amplifies the meaning and the complexity of the term privacy, also exposing health institutions to new kinds of vulnerabilities. Regulations are key interventions in this context, with supernational entities like European Union having a common, broad and complex framework (GDPR) and – in general – a significant disparity among the countries in the world. However, addressing these threats cannot be solely based on legal means, since a fruitful approach should include also IT and risk management strategies, together with the compliance with standards such as ISO 31000. Prevention and management of cyber-risk in healthcare requires a multidisciplinary approach; in our digital culture healthcare professionals (as well as administrative staff involved in healthcare) need to be trained specifically in cyber security in order to avoid damages. Therefore, is nowadays anachronistic to assume that a Medical Expert may be just proficient in medicine in order to perform a correct service in management of a healthcare organisation and a solid digital expertise should be required for healthcare experts who work in central structures and who device operative working procedures.

[77] D.J. Hunter and R. Bengoa, *Meeting the challenge of health system transformation,* in *European countries*, in *Policy and Society*, vol. 42, issue 1, 2023, 14–27.

[78] B. Gaudenzi, *Il Risk Management nelle aziende sanitarie*, in *Rivista Italiana di Medicina Legale e del Diritto in Campo Sanitario*, vol. 4, 2020, 1997-2011.

[79] ISO (2009) International standard: risk management: principles and guidelines. ISO 31000. Principes Et Lignes Directrices. ISO.

[80] M. Ferdosi, R. Rezayatmand and Y. Molavi Taleghani, *Risk Management in Executive Levels of Healthcare Organizations: Insights from a Scoping Review (2018)*, in *Risk Manag. Health Policy*, vol. 13, 2020, 215-243.