RAIS Journal for Social Sciences | VOL. 5, No. 1, 2021
ISSN 2574-0245 (Print) | ISSN 2574-1179 (Online) | DOI: 10.5281/zenodo.4782466

Security and Privacy in the Era of Electronic Health Records (EHRs)

Mohamed CHAWKI

Ph.D., FRSA, Chairman, International Association of Cybercrime Prevention (AILCC), Paris, France
chawki@cybercrime-fr.org

ABSTRACT: Traditional paper-based repositories of medical records are now largely phased out and replaced by advanced Electronic Health Record (EHR) systems. Digitization of medical records and the ease of data access, however, also present the risk of the healthcare data breach and misuse of personally identifiable information. Given the crucial data kept in EHR, specific regulations are made in the European Union (EU), which specify the amount and type of clinical data collected. In various countries in the EU, however, the amount and the nature of the EHR information are different. Some EU countries allow the collection of minimal demographic and clinical information. In contrast, others allow more specific information on the profession, criminal offense, organ donation, psychological disorders, family details, or other socio-economic variables. Security of individual data has been identified as a fundamental right in Article 8 of the EU Charter of Fundamental Rights, and the EU General Data Protection Regulation (GDPR) dictates that organizations can analyse individual information only if a minimum of a sixth lawful grounds for personal information processing has complied. These requirements become even more stringent in medical data. One of the main issues for EHRs is how patient's privacy will be kept confidential through technology. Another primary concern is network communication; thus storing personal health data online can be a source of crucial information leakage to unauthorized entities. In detail, this study seeks to analyse and address the following issues: Firstly, an overview of security and privacy concerns in EHR will be looked into details. Secondly, an analysis of the existing legislative and regulatory framework to protect the treatment or processing – including collection, recording, organisation, structuring, storage, and other uses – of personal data linked to health will be provided, taking the European Union as a case study. The paper will conclude by discussing that with the recent advances in data storage and data processing and the emergence of artificial intelligence and big-data projects, EHR applications are expected to grow further. The need is to strengthen further and homogenize the regulatory framework for the security of data stored in EHR and the standardized analysis of information for legitimate clinical research and other essential applications.

KEYWORDS: Medical Health Record (EHR), Privacy, Security, European Union (EU), General Data Protection Regulation (GDPR)

> "If you need to be persuaded that you're living in a science-fallacy world, look at your mobile phone."
> *Bruce Schneier*

Introduction

Before the digital age came about, processing health data did not present the complex issues that it does today. Indeed, it was attached on a critical trust of connection between the invalid and the medical experts, who in various instances would be the GP. Back then, everything was written down on paper, if not spoken merely (Guarda 2009, 1).

The arrival and various distribution of communication gadgets like computers resulted in various issues and increased need for security. Modern technology has introduced gurus with the fantastic workforce to accede wide length of aggregated information ever so rapidly while also enabling people to create massive databases which various people – even if lower in figure and categorically identified – can accede (ibid). This has majorly accelerated the dangers accompanied with how such data is processed, including its unlawful circulation and dissemination, which can directly impact the dignity and the greater freedoms and rights of the one's data subject (ibid).

Indeed, the use of data has faced ethical and legal problems in all areas of health treatment. It is known that patients can quickly get helped by possessing medical health data, and medical decisions greatly enhanced through a detailed understanding of medical history and health / medical data (Esteve 2018, 36). Nevertheless, we need to guarantee confidentiality – including the right to protect data – and confidentiality to patients associated with health data processing problems from important rights dimension (ibid).

The General Data Protection Regulation (GDPR) recognizes "data *containing medical information'* as a crucial type of data, and to this end, enhance a meaning of health data for data protection function (edps.Europa.eu, 2020). While the innovative idea brought by the GDPR (such as confidentiality by design or the illegality of discriminatory profiling) remain crucial and functional to medical information, calorically protection for individual health data have now been addressed by the GDPR (ibid), enabling there to be a definitive understanding of the rules which, in turn, guarantees proper and elaborate protection of such information. Processes that fasten realisation of new ideas and better standards health protection, like clinical trials or *mobile medical,* require strong data security information to maintain trust and confidence through regulations to protect their data (ibid).

Since Electronic Health Records are still somewhat new, there was some difficulty finding many studies performed on them' legal risks. All of the articles used in this paper were extremely relevant to the topic; however, not all of them deal with the research problem.

It is fundamental consideration that EHR is increasingly actioned in several developing countries as it improves the standards of medical care and is cost-efficiency. In Saudi Arabia, a systematic review revealed that lack of computer experience and lack of perceived usefulness are major barriers in the successful implementation of EHR (Alqahtani et al. 2017, 14). These findings indicate that such digital ideas can initiate dangers in the absence of an efficient policy and technical framework. Therefore, it is a perfect shortcoming to protect the data safety that are stored in the programme. Protection ineffectiveness has of late raised questions about this system (Keshta and Odeh 2020, 2).

Although it is gaining ground and becoming more practical, and there an increasing vigour for its adoption, minimal consideration has shown indications to the protection and confidentiality challenge that could increase as an effect. Therefore, the author has done a detailed research of all the significant problems related to the EHR system's security and privacy properties as indicated in the public scholarly literature taking the European Union as a case study. Literature has shown that EHR outcomes received from several merchants always come with automatic security and confidentiality affordability. The current concern could receive a positive respond by studying the targeted pure results used as EHRs. Furthermore, the author believes that if the security and privacy overtures contained in the published scholarly literature are pointed out and well searched, they can continuously be used as a substitute for what can be the absolute EHR security and privacy overtures. The study is likely to reveal essential data for the custodian in health facilities and various stakeholders required to act, identify, develop and apply various Electronic Health Records which improve the confidentiality and protection of the invalid who participate. The current study is as well useful for stakeholders who oversee information systems' security and confidentiality within the medical care department. The study can as well be utilized by other researchers as a reference on how the patients' privacy and security can be improved in the electronic medical data bases.

The remaining part of the study will be done as follows. Section 1.1 presents medical information be incorporated in EHRs. Section 2.1 discusses concerns of privacy and security of EHRs. Section 3.1 focuses on the EU Charter of Fundamental Rights (EUCFR) and the EU General Data Protection Regulation 2016/679 ("GDPR"). Section 4.1 will discuss numerous procedures which are adopted in EHR systems to receive security and privacy. Finally, the author concludes by discussing that with the recent advances in the keeping and processing of information and the emergence of artificial intelligence and big-data projects, EHR applications are expected to grow further. The need is to strengthen further and homogenize the regulatory scheme for the data protection stored in EHR and the standardized processing of information for legitimate clinical research and other essential applications.

1.1. Health data to be included in EHRs

The electronic processing of health data provides invaluable benefits to patients and health care providers. These benefits include speed and flexibility of information processing, retrieval, and communication; long-term cost savings due to increased efficiency; and the availability of powerful computational techniques that can contribute to improved patient outcomes (Hoffman and Podgurski 2007, 332). Burton et al. suggested that EHR can be of great help in delivering coordinated medical care for patients with multiple chronic conditions (Burton et al. 2004, 458). Moreover, if fully adopted, EHRs will be internally utilized, allowing disparate systems and networks to send and receive data across the country. They will be vertical, including all of the persons' health care encounters over a long period. They also will be extensive, comprising the records of all visits with doctors and other health care providers, such as dentists, chiropractors, and specialist therapists (Rothstein 2007, 487).

They are identifying the kind of data that is contained in EHRs requiring proportional competing interests. In another way, extensive EHRs gives a better outlook of the invalid's health (European Commission 2014). Allowing health experts to produce a well replicated diagnoses and health feedback to invalids. Medical data in EHRs, which is readily reached and interpreted than data on paper-records, could be susceptible (e.g., data containing information about diseases transmitted sexually, mental disorders, drugs or alcohol dependence). The feature gets solid consideration under EU law (ibid). The Charter of Fundamental Rights accepts every individual's right of security to personal information and privacy, and Directive 95/46/EC afford exquisite security to medical information. The general regulation in this Directive that information gathered has to be 'fulfilling, show relevance though not exaggeration concerning the function with which they are gathered for further processing and particular relevance to explaining that information has to be incorporated into EHRs (ibid).

Many European countries, exceptional of local administration information on the sick person which includes name, gender, date of birth and national insurance number need that just medical information is entailed in EHRs. Bulgaria, Luxembourg, France, and Italy accept that data can be included on EHRs about the invalid transplanting of body parts (ibid).

Additionally, in various European states, EHRs are never restricted to health information. The extra information which needs to be added in EHRs is extensive. This information contains more individual information starting with the profession, then health habits and also criminal offenses (ibid).

EHRs in Croatia have to incorporate data on the insured individual's duty and career-related information and certain acts of smoking, alcohol drinking, and dependence on substances. The Danish details invalids' keens. The EHRs in Estonia contains the invalid's career and employer, describing the workings standards, educational background, the state of the family, health habits, psychosocial background and development, mental background, and development. EHRs in France contain a part on prevention that protects medical and social details. In Greece, health data comprises of the father's details and the patient's career (ibid). In Hungary, the career of the invalid has to be incorporated. The Italians include, also to health information, social and medical information.

Nevertheless, no proper definition of this study entails is explained. In Luxembourg, the legal rules accept the patient to fill a section of the EHR where he/she can produce extra data or agreement. In Slovenia, the marital status, education, and profession of a patient have to be encompassed in EHRs. In Spain, the occupation of a patient is involved. Sweden accepts data to be covered about criminal offenses of a patient only when there is a definite necessity to perform. Romania is analysing the likelihood of including in the EHRs data on religion, job tittle, lifestyle/behaviour, family periodical information (ibid).

2.1. Concerns on privacy and security of EHRs

Privacy and security are the primary aim for growing personal trust and information improvement. There can't be privacy in the absence of security practices (Lafky and Horan 2011, 68). The health data of invalid's/persons should be safe and confidential within the medical assistance professional and individual and forgetting a healthier outcome (Tanwar et al. 2019, 8). The invalids are slow to open his/her medical detail he/she does not have trust in the EHR system. Hence, health records' privacy and security play a fundamental function because the exposure of the medical information of invalid could create life-threatening feedback.

Research done in a Taiwanese hospital reported that, concerning data privacy, invalids' interests in gathering data about themselves, another function of this data, and the somehow drawback in the recorded data were associated with their information privacy-protective feedback, while concern for illegal access to their data by other staff in the healthcare facility was not (Kuo et al. 2013, 23).

Security and confidentiality are needs between patients and physicians/doctors. The EHR produces medical information from numerous data sources like patient's warbles, smartphones, caregivers, in-invalid care, PHR system, and so on. Generally, patients can control the access of their EHR, but they cannot add additional data (Mense et al. 2014, 241).

Many studies conclude that to obtain the full potential of EHRs, patients should be able to access them anywhere and anytime. If EHRs are accessible, patients can verify the details and make a more informed assessment of their health status (Alanazi and Anazi 2019, 107). In a study from United Kingdom, it was found that patients could indeed identify a range of inconsistencies in EHR, and improve the data accuracy (Freise et al. 2021, 6). Efficacy of EHRs can be further enhanced by making them portable, turning them into Personal Health Records (PHRs) (Huang et al. 2009, 748); a solution is to keep PHRs in portable storage media such as USB flash drives. This portability adds an additional mobility feature whose security needs to be covered; it is necessary to prevent the data from being exposed (Tejero and de la Torre 2012, 3020). However, in a study on 13 USB-based PHRs, several deficiencies with respect to technical features and clinical data elements were observed (Maloney and Wright 2010, 97). These authors, therefore, recommended tethered or web-based PHRs as better alternatives to USB-based PHRs.

Once information is produced, it is kept in the local databank and then keep at the remote system using a remote gateway. Immediately after data collection, they get stored it and more share it, the likelihood of attacks and confidential issues start here (Tanwar et al. 2019, 8).

There are several recent examples of the detrimental effect of cyber-attacks on healthcare institutions and patients (Beavers and Pournouri 2019, 251, Seh et al. 2020, 133). The 2017 WannaCry ransom ware attack, which affected the UK National Health Service (NHS), demonstrated the lack of readiness for protecting patient data and health delivery systems, despite the sector not being specifically targeted (O'Brien et al, 2020). Similarly, attacks across healthcare organizations and systems in numerous countries have compromised patient records and shut down services. Furthermore, deployment of EHR system on large scales, makes it necessary to implement a policy and technical framework that can mitigate the risk of a potential EHR failure in the event of some natural or man-made disaster (Sittig and Singh 2012, 1854). Despite increasing cyber threats and multiple cyber-attacks, evidence reveals that healthcare systems worldwide are still lagging behind other critical sectors in responding to this challenge (O'Brien et al. 2020). Following the emergence of the Covid-19 pandemic, there has been an increase in the number of cyber-attacks globally against healthcare organizations, making it increasingly important that healthcare institutions understand and develop their cyber security, planning and preparedness (ibid).

To initiate this, several security preservation techniques must be applied. A part of privacy skills includes, access control model, grant access, and pseudonymity. Moreover, there include attack mitigation techniques like authorization and authentication. In this respect, blockchain-based strategies can be effective in maintaining a balance between security and ease of access (Ramachandran et al. 2020, 343). To be restored from illness, the invalid has to provide their data like blood pressure, height and weight, previous medical history with physicians to diagnose the ailment and act rightfully for treatment. In some situations, patients who have psychiatric disorders or HIV, find it challenging to disclose because it could result in social scrape and prejudgement (O'Brien et al. 2020). Furthermore, the current medical details of patients, resultantly collection of further data is required which includes the patient's identification for example, past medical judgment, individual history, digital representation of medical images, formerly healthcare assistance taken from which physicians, medicinal history, inherited disease details, genetic disease history the likes of haemophilia, diet-habits, psychological outlines sexual dependence, history of employment, and income, emotional and mental conditions including others (ibid).

Whetstone & Goldsmith confirmed that a person's confidence in their medical records' privacy and security had a good impact on their psyche to develop an electronic medical information (ibid). Bansal et al. ascertained privacy regards not positively influenced the willingness to disclose their medical data online (ibid). Further survey done by Anderson & Agarwal discovered the extreme effect health data security interests that intending persons cooperate in giving personal health data (Keshta and Odeh 2020, 4). Moreover, Dinev et al. discovered a worse interaction between people's health data confidentiality, resulting attitude following electronic medical data. Angst &

Agarwal came up with a similar ending concerning the adoption of digital medical records. Research carried out by Ermakova et al. revealed that interests in medical data confidentiality lowered patients' intentions allowing medical practitioners share their health information during application of cloud computing techniques (ibid).

The occurrence of confidential interests makes confidence trivial compared to rations when selecting medical care except for a less than primary use. Kuo et al. conducted a research, its outcome approved prevailing concerns on medical data confidentiality on the information privacy-protective responses (IPPR) the likes of the refusal of patients to provide their data to medical practitioners, synthesizing individual data of patients to health centres, seeking withdrawal of individual data of invalids, discouraging responses to their friends, feedbacks delivered directly to health institutions, feedbacks delivered indirectly to a third-party organization (ibid).

Rohm and Milne concluded that consumers' interests rose when an agency got a list comprising personal health records in comparison to a form having the general information. Research by Zelman et al. said that persons' choices concerning sharing their electronic health details, whose variation depends on the type of data subjected to the public. King et al. also noticed concerns regarding privacy differ in various forms of medical history. It was affirmed that concerns in medical centres that human beings are interested in the inability to conceive children, abortion, STDs, and much more issues that exactly impact their families. Individuals expressed reduced privacy interests in the health information they delivered about religion, date of birth, blood group, language, gender, and cancer status blood pressure status (ibid).

3.1. European Union legal framework

At the European Union Law level, we will focus on the EU Charter of Fundamental Rights (EUCFR) and the EU General Data Protection Regulation 2016/679 ("GDPR")

The EU Charter of Fundamental Rights (CFR)

The EUCFR is keen on the principle of human dignity (Article 1), the right to life (Article 2), the right to the integrity of the person (Article 3), the prohibition of torture and inhuman or degrading treatment or punishment (Article 4), respect for private and family life (Article 7), protection of personal data (Article 8), the prohibition of all discrimination including that of genetic characteristics in an expressway (Article 21).

It is notably rightful to outline Article 3 EUCFR, as it adheres to everyone's right to respect his or her physical and mental integrity. Article 3(1) states that "*in the fields of medicine and biology, the following must be respected in particular*" (Article 3(2) "(a) the available and informed knowledge of interested individual, regarding to the methods underlain by legal act; (b) Proscription of eugenic actions, most importantly those targeting the selection of persons; (c) Disallowing formation of the human body and its organs a source of financial advantage; (d) Forbidding the reproduction of an exact copy of people."

Yet the EU Charter is well renowned human rights tool that upholds inclusivity of the necessary generation of rights, that cannot be avoided because they give the raised standard of protection for ground laying rights, that entails, just as other human rights tool, a safeguarding clause in article 53, ruling that: "*Nothing in this Charter shall be interpreted as restricting or adversely impacting human rights and fundamental freedoms as recognised, in their various fields of application, by Union law and international law and by international agreements to which the Union or all the Member States are party, in addition the European Convention for the Protection of Human Rights and Fundamental Freedoms, and by the Member States' constitutions*."

Nonetheless, the European Court of Justice explained article 53 not in a safeguarding manner. The provision cannot permit a Corporate State to apply for the national ground laying rights standard (EU law scope). This is possible when the EU law stipulates to be done assuming the primacy of EU law. Resultantly, the EU standard of security will bind as a generic rule when under the jurisdiction of EU law, which cannot be avoided (Esteve, 2018, p.47).

The EU General Data Protection Regulation 2016/679 ("GDPR")

On May 25, 2018, the General Data Protection Regulation (GDPR) took full legal effect across the European Union (EU) and, subsequently, the European Economic Area (EEA), which together comprises 31 countries (Dove, 2018, p. 1013). It is solely applied in all corporate states of the European Economic Area ("EEA") and applies to companies within and outside the EEA in most cases where either the controller, processor or the information subject is based in the EU (Determann, 2020, p. 240). According to the EU data protection law, organizations must not process individual information unless they can justify expressly recognized by law. EU lawmakers reversed the general presumption of liberty (everything is allowed if it is not prohibited) for the field of data processing and data protection law; now, absorption of individual information is not allowed if not permitted.

According to the GDPR, organizations must not process personal data unless they meet all requirements of the legal rules and state laws, and they can claim one of six "legal bases": (a) the information subjected is due consent to process their individual information for various specific reasons; (b) Synthesis of information is critical for the effectiveness of an agreement to which the subjected information is prompted to take steps at the need of the subjected information before it enters into an agreement; (c) processing is essential for adherence to lawful duty of which the controller is subject; (d) synthesis is needful to secure the critical concerns of subjected information or other mortal human; (e) processing also helps the performance of a duty conducted in the public interest or the action of legal power vested in the controller; (f) also processing is fundamental for legitimacy concerns advised by the manager or by a third party, excluding concerns are controlled by concerns or crucial rights and freedoms of the data conditioned that need the security of individual information data (ibid).

Concerning health data, which is termed in European law 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," the regulation is even more complicated, and there are further restrictions. Health data is grouped as a "special category" as described in Article 9(1) of the GDPR, regardless of how sensitive information about one's health is; for example, glasses or a Band-Aid visible on security footage or scanning of a public road by an autonomously-driving car will turn the entire data set into one containing "special categories of personal data," because they contain information on person's health. Processing of health data is prohibited not only if the data conditioned has given her clear consent for various specified reasons or the processing is needed for health or medical reasons, in which scenario the data could be "processed by or under the responsibility of a professional subject to the obligation of professional secrecy" without consent (ibid).

Consent plays a vital role in containing patients' privacy. A sought consent means that a patient is completely aware of the implications of their medical status and voluntarily agrees to divulge or permit access to a collection of their health data (Win, 2005, p. 13).

For medical research, Article 9(2)(j) and Article 89 of the GDPR contain several exceptions to the general rules concerning consent and access rights while still requiring certain safeguards. Notably, GDPR explicitly mentions that minimal information should be preserved within EHR or similar records (Chassang, 2017, p. 709). Articles 9(2)(h), 9(2)(j), and 89 of the GDPR allow EU Member States to legislate additional derogations from several provisions of the GDPR concerning the rights of data subjects. For example, in Germany, Article 22 the latest German Federal Data Protection Act (Bundesdatenschutzgesetz) ("BDSG") names several exceptions from the GDPR requirements for processing data of a particular category. Such processing is allowed in Germany, for example, for social security administration purposes and preventive medicine and public health interests and prevent public harm. Simultaneously, various necessary safeguards are described in Section 2 of the BDSG, pseudonymization being one of them. Also, Article 27 of the BDSG justifies a limitation on the data subject's rights under the GDPR if the data synthesis is essential for research purposes. The concerns of the controller outweigh those of the data subject. However, in addition to the safeguards already mentioned in Section 22 of the BDSG, distinguished groups of individual information have to be anonymised as soon as possible after being processed for their original purpose. The leeway granted to the EU Member States to legislate derogations from the GDPR enables creating a legal patchwork that makes it more difficult for research institutions and companies to conduct international studies or exchange data across borders. In addition to data protection laws, treating physicians and researchers must comply with Regulation (EU) 536/2014 on Physiological Tests on Medicinal Products for Human Consumption, which standardizes authorization procedures, safety necessities, and consent requirements to participate in clinical trials. This further complicates the preparation of consent forms and adds restrictions to the subsequent use and sharing of information derived from clinical trials (Determann 2020, 240).

4.1. Solutions for EHR development

We understood an EHR system in previous sections and tabled the significant concerns on this system's privacy and security. In this part, we will discuss various procedures used in EHR systems to attain security and privacy.

Encryption Techniques

EHR systems choose if to preserve the data in the systems in decrypted or concealed form. Although it is necessary that to preserve trust, privacy and data integrity, it has to be kept in conceal. There are two methods for information obscurity, which are similar and dissimilar schemes. The challenge with dissimilar communication security is, it is incredibly inefficient, primarily in health records regarding data imaging. Furthermore, they have cognitive issues when there is a need to search or hide labels. Hence, high preference for symmetrical cryptography. It is solved by using a hybrid public critical infrastructure (HPKI) suggested by Hu et al. The infrastructure is HIPAA reliable. Adopts critical public infrastructure for reliability, yet computing does not require intensive information and a better effective symmetric mechanism for information imaging. Also, the computation of encryption of medical information having images requires more work, time-consuming, and expensive. Energy has been inputted to handle this matter. Kanso and Ghebleh suggested ideas that employ robust and specific conflict-oriented image encryption mechanisms. The technique comprises various rounds, comprising of double phases which include, preserving and changing phase. For efficiency and maintaining security, a pseudorandom matrix is employed. Other biometric techniques have reliable solutions when it comes to encryption. Although, there is susceptibility to breach for servers containing the encryption. The first is to conserve a separate server for information and the proper keeping key so they are not subjected to breach. Secondly, do away with crucial storage in servers by enabling invalids in creating and maintaining their keys. Various mechanisms of encryption schemes provide access control, like identity-based encryption. The database standard techniques for encryption like transport layer security (TLS) are employed to safely transport data over the Internet, thereby avoiding information spoofing or person –at- the- center conflicts (Tanwar et al., 2019, p. 100).

Access Control

Handling legal and access control provides the most critical challenge in the creation of EHR systems. EHR systems, if properly designed, can have explicit access rules (Bakker, 2004, p. 267). Firstly, the two primary ways to solve this challenge are to incorporate keeping the data in the centralized system under the team's privacy handling systems. Access control procedures are utilized to produce the finest level of access 100 privacy and security of electronic medical care data and authorization in such cases. These techniques keep data whose format is not encrypted since the access control serves as a firewall protecting the server from illegal access. Also, it's to combine the obscurity of data and access controls that lead to legal access and integral data thereby availing security and privacy to the information kept in encrypted method. This can be made functional by putting into use the utilization of the Cryptographic Access Control Model. This brings ways for building solid EHRs comprising of data from several sole sources (Tanwar et al., 2019, p. 100).

Digital Signature and Verification

Present signatory mechanisms are essential for producing reputable, integral and authentic present files. Zhang et al. employ the use of relevant signatories (ibid). The importance of two signatory techniques in EHR systems shall be discussed, that is anonymous signatories and threshold signatures.

Anonymous signatures

To store the participant's identity and ensure confidentiality, methodologies for releasing pseudonym identifiers are put into use. In this regard, a pseudonymization-based system was proposed to secure EHR architectures (Riedl et al, 2008, p.1). This system proposes the use of transport layer security or signed messages to enhance the security of EHR. However, anonymous signatures allow masking in the signatory scheme. There are various mechanisms for having unidentified signatories, explored into detail two of these significant ones: (1) ring signature and (2) group signature.

Group signature: This was incorporated by Chaum and Van Hejst (Tanwar et al., 2019, p. 104). The mechanism entails a team of participants led by a team leader that gives a go-ahead to participant among them to provide a signatory on behalf of the group participant homogenously. The leader's role is monitor participant joining and reshuffling procedures. Additionally, the leader can also interfere with signatories if the case is disputed. Each group participant has a different confidential signing key, and only one public key, which could be used by a third party to check if the signatures of the group has been signed. Privacy and security of electronic medical care information Any group participant can sign in the group participant's absence, and it will not affect the singer's identity. Every group participant must have a durable identity attached to the group and the participants ' secret key. The interaction, nonetheless, is a secret to the group leader.

Ring signature: This was brought about by Tauman, Rivest, and Shamir (ibid) to disclose private data without enclosing who signed the message. The scheme's agenda is identical to that of the group signature scheme: to conserve identity of the signer masked by the group. Reviewing checks signature's legality without knowing who initiated it from the likely ring member. Furthermore, double signatures produced by a similar signer are not likable—the two key variations between group and ring signatory mechanisms. Firstly, lack of a mechanism to restore signatories in ring signature schemes. Secondly, it is not helpful to program people in the ring signature scheme, which is several participants can operate in unison for a mechanism avoiding preambles.

Threshold signatures

The bottom-most mechanism (ibid) needs that every system containing members that encrypt or decrypt information requires a minimum member's participation. Also, to say, an optimum signature is a unique method of dealing with numerous statutory. At least a few populations need to produce a divide of signatures to provide a singlet signatory to members. Both private and public key pair is what makes up a group, made accessible to members. Shamir's private sharing mechanism is a bottom-most technique that enables members to be confidential in sharing from. A private sharing doesn't reveal data regarding the initial secret, thereby not function independently. Boneh, Lynn, and Shacham (BLS) (ibid) mechanism absorbing Shamir's secret sharing enhances the system of crucial generation required to provide keys employed during signing and verification of data conducted in distributed measures doing away with concerns of one-person member to be confided in. It is a compelling feature because the initial secret should not be available. These private shares can provide their signatures only when they validate against their public key. Nevertheless, there is the ability to gather various numbers of these signature shares and extrapolation carried out for confidential shares. In that scenario, we can restore the signatories created when the original key had been used (ibid).

Conclusions

This article provided a brief account of complexities associated with the recording, accessing, and processing EHRs in the EU. Since EHR contains compassionate and personally identifiable information, data breach prevention is given the highest priority. Indeed, the protection of personal data has been identified as one of the fundamental rights in the EU, and considering the sensitivity associated with medical health records, the access and processing of EHR is permitted only under exceptional circumstances. Consent of the patient and overriding medical benefits are two requirements for the processing of EHR. The EU, however, permits the Member States to make nation-specific legislation on some of the provisions of GDPR, leading to differences in the practices and protocols related to the processing of EHR. These deviations complicate the compilation and processing of medical data for multinational clinical trials and medical research.

Notwithstanding such complexities, EHRs play a critical role in providing better and timely care to patients and advancing medical research. In the coming years, the volume of EHR and the scale of medical data processing are expected to increase phenomenally. Despite such challenges, EHR has been instrumental in providing better patient care and fostering medical advances. With the recent advances in data storage and data processing and the emergence of artificial intelligence and big-data projects, EHR applications are expected to grow further. The need is to strengthen further and homogenize the regulatory meshwork for the security of information stored in EHR and the standardized synthesis of information to legitimate clinical survey with other vital applications. It is essential to augment the legal and regulatory framework so that the data can be accessed to better humanity while safeguarding the privacy of personally identifiable information.

References

Alanazi, Abdullah and Yousif Al Anazi. 2019. “The Challenges in Personal Health Record Adoption.” *J Healthc Manag* 64(2): 104-109.

Alqahtani, Asma, Richard Crowder and Gary Wills. 2017. “Barriers to the Adoption of EHR Systems in the Kingdom of Saudi Arabia: An Exploratory Study Using a Systematic Literature Review.” *Journal of Health Informatics in Developing Countries* 11(2): 1-23.

Bakker, Ab. 2004. “Access to EHR and Access Control at a Moment in the Past: A Discussion of the Need and An Exploration of the Consequences.” *International Journal of Medical Informatics* 73(3): 267-270.

Beavers, Jake and Sina Pournouri. 2019. “Recent Cyberattacks and Vulnerabilities in Medical Devices and Healthcare Institutions”. In Hamid Jahankhani, Stefan Kendzierskyj, Arshad Jamal, Gregory Epiphaniou, Haider Al-Khateeb (Eds.), *Blockchain and Clinical Trial*, Springer, pp. 249-267.

Burton, Lynda C., Gerard F. Anderson and Irvin W. Kues. 2004. "Using Electronic Health Records to Help Coordinate Care." *Milbank Q* 82(3): 457-481.

Chassang, Gauthier. 2017. “The Impact of the EU General Data Protection Regulation on Scientific Research.” *Ecancermedicalscience* 11: 709. doi: 10.3332/ecancer.2017.709.

Determann, Lothar. 2020. “Healthy Data Protection.” *Michigan Technology Law Review* 26(2): 229-278.

Dove, Edward. 2018. “The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era.” *Journal of Law, Medicine & Ethics* 46: 1013-1030.

Esteve, Joaquín. 2018. “Health Data Treatment. An Approach to the International and EU Legal Framework.” In *Genetic Information and Individual Rights*, Series "Law & Science" Vol. 1, edited by Arnold R., Cippitani, R., Colcelli V., 36-53. Universität Regensburg, Regensburg.

European Commission. 2014. “Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services.” Available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf. Accessed 9/10/2020.

European Data Protection Supervisor. Available at edps.europa.eu. Accessed 7/10/2020.

Freise, Lisa; Neves, Ana Luisa Neves, Kelsey Flott, Paul Harrison, John Kelly, Ara Darzi, and Erik K Mayer. 2021. "Assessment of Patients’ Ability to Review Electronic Health Record Information to Identify Potential Errors: Cross-sectional Web-Based Survey.” *JMIR Formative Research* 5(2): e19074.

Guarda, Paolo. 2009. “Electronic Health Records: Privacy and Security Issues in a Comparative Perspective” (December 26, 2009). Available at SSRN: https://ssrn.com/abstract=1528461.

Hoffman, Sharona and Andy Podgurski. 2007. “In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information.” *Boston College Law Review*, Vol. 48, No. 2, March 2007, Case Legal Studies Research Paper No. 06-15, pp. 331-386. Available at SSRN: https://ssrn.com/abstract=931069.

Huang, Lu-Chou, Huei-Chung Chu, Chung-Yueh Lien, Chia-Hung Hsiao, and Tsair Kao. 2009. “Privacy Preservation and Information Security Protection for Patients’ Portable Electronic Health Records.” *Comput Biol Med* 39(9): 743-750.

Keshta, Ismail and Ammar Odeh. 2020. “Security and Privacy of Electronic Health Records: Concerns and Challenges.” In *Egyptian Informatics Journal,* Online, available at https://www.sciencedirect.com/science/article/pii/S1110866520301365?via%3Dihub. Accessed 21/12/2020.

Kuo, Kuang-Ming, Chen-Chung Ma, Judith Alexander. 2013. “How Do Patients Respond to Violation of their Information Privacy.” *Health Information Management of the Health Information Management Association of Australia* 43 (2): 23-33.

Lafky, Deborah and Thomas Horan. 2011. “Personal Health Records: Consumer Attitudes Toward Privacy and Security of Their Personal Health Information.” *Health Informatics Journal* 17 (1): 63-71.

Maloney, Francine and Adam Wright. 2010. “USB-based Personal Health Records: An Analysis of Features and Functionality.” *Int J Med Inform* 79(2): 97-111.

Mense, Alexander, Franz Pfortner, and Stefan Sauermann. 2014. “Security Challenges in Integration of a PHR-S into a Standards Based National HER.” *Studies in Health Technology and Informatics* 205: 241-245.

O'Brien, Niki, Guy Martin, Emilia Grass, M. Durkin, Ara Darzi, and Saira Ghafur. 2020. “Cybersecurity in Healthcare: Comparing Cybersecurity Maturity and Experiences Across Global Healthcare Organizations.” Available at SSRN: https://ssrn.com/abstract=3688885.

Ramachandran, Shwetha, Obu Kiruthika, Aishwariyavalli Ramasamy, R Vanaja, and Saswati Mukherjee. 2020. “A Review on Blockchain-Based Strategies for Management of Electronic Health Records

(EHRs).” *International Conference on Smart Electronics and Communication (ICOSEC),* IEEE, pp. 341-346.

Riedl, Bernhard, Veronika Grascher, Stefan Fenz, and Thomas Neubauer. 2008. “Pseudonymization for Improving the Privacy in E-Health Applications.” *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, pp. 1-10.

Rothstein, Mark. 2007. “Health Privacy in the Electronic Age.” *J Leg Med* 28 (4): 487-501.

Seh, Adil Hussain, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. 2020. “Healthcare Data Breaches: Insights and Implications.” *Healthcare (Basel),* 2020 June 8(2): 133.

Sittig, Dean and Hardeep Singh. 2012. “Electronic Health Records and National Patient-safety Goals.” *N Engl J Med* 367(19): 1854-1860.

Tanwar, Sudeep, Sudhanshu Tyagi, and Neeraj Kumar. 2019. “Security and Privacy of Electronic Healthcare Records.” *The Institution of Engineering and Technology*.

Tejero, Antonio and Isabel de la Torre. 2012. “Advances and Current State of the Security and Privacy in Electronic Health Records: Survey from a Social Perspective.” *J Med Syst* 36 (5): 3019-3027.

Win, Khin. 2005. “A Review of Security of Electronic Health Records.” *Health Information Manag.* 34 (1): 13-18.

Bio-note

Mohamed Chawki holds a Ph.D. in law from the University of Lyon III in France for a dissertation on French, British and American cybercrime legal systems. This was followed by a 3-year post-doctoral research in cybercrime at the Faculty of Law, University of Aix-Marseille, France. He is a Senior Judge (Egypt), a Fellow of the Royal Society of Arts (UK) and the Founder Chairman of the International Association of Cybercrime Prevention (France). He was awarded the Presidential Medal of Excellence in 1998 (Egypt), and the Distinguished Services Medal in 2009 (Brazil).