TECH HIVE ADVISORY

IKIGAI

DEPLOYING ELECTRONIC HEALTH RECORDS FOR MEDICAL RESEARCH

About Tech Hive™

Tech Hive Advisory Limited ("Tech Hive") is a technology policy and advisory firm that provides advisory and support services to private and public organisations regarding the intersection between technology, business, and law. We focus on how emerging and disruptive technologies alter and influence the traditional way of doing things while acting as an innovation partner to our clients.

Our experience and capability extend across Research and Policy Advisory, Privacy and Data Protection, Data Ethics, Cybersecurity, Start-Up Advisory, and Digital Health. We ensure our advice serves our clients well by understanding their business and the markets they operate in through accurate policy and legislative development tracking and intelligence.

Contact: contact@techhiveadvisory.org.ng

About Ikigai™

Ikigai Innovation Initiative is a non-profit organisation set up to become the one-stop centre for technology policy in Africa. We promulgate diverse research on technology policy and legal frameworks across Africa. We also engage relevant stakeholders around the intersection of law, business and technology and advocate for better policies for the ecosystem. Being an advocacy centre focused on emerging technologies, policy, and research, we often work and collaborate with leading research institutes, academia, organisations, civil society, and individuals on technology policy. We also publish and contribute to whitepapers, reports, policy briefs, infographics, guides and guidance, academic journals and publications.

Our researchers work closely with government, stakeholders and ecosystem players, placing evidence and academic intuition at the heart of policymaking. We bring together the latest insights, evidence and commentary from our researchers with our one-stop-shop vision for policy by connecting policymakers, decision-makers, and practitioners with our industry- leading research. We also deliver evidence-based policy that meets the grand challenges facing society by advocating for social justice in the face of technology, sensitising the public
on technology policies that impact their rights and lives, and promoting digital rights and digital ethics.

Contact: policy@ikigaination.org

Author

Sandra Musa

Disclaimer - Usage of Paper

The Paper is general and educational and is not intended to provide, and should not be relied on, as a source of legal advice. This information and material provided in the Paper may not be applicable in all (or any) situations. Accordingly, it should not be acted on without specific legal advice based on particular circumstances.

However, specialist advice should be sought about readers' specific circumstances, and we are available to provide expert advice on the specific circumstances when they arise.

Tech Hive Advisory (Tech Hive) and Ikigai Innovation Initiative (Ikigai Nation) believe that the information it uses comes from reliable sources but do not guarantee the accuracy or completeness of this information, which is subject to change without notice, and nothing in this document shall be construed as such a guarantee.

Neither Tech Hive, Ikigai Nation, nor any of their officers or employees, including the contributor, warrant or represent the accuracy or completeness of the information set out in this Paper. Such ideas or recommendations reflect the different time frames, assumptions, views and analytical methods of the person who prepared them. Tech Hive and Ikigai Nation are under no obligation to ensure that such other ideas or recommendations are brought to the attention of any recipient of this Paper.

Tech Hive and Ikigai Nation disclaim any liability arising from using this document or its contents.

Users of this Paper should determine whether they agree with the content.

The absence of any trademark or service mark from this list does not waive Tech Hive's and Ikigai Innovation Initiative's intellectual property rights in that name, mark, or logo.

The absence of any trademark or service mark from this list does not waive Tech Hive's and Ikigai Nation's intellectual property rights in that name, mark or logo.

Abbreviations

CAGR - Compound Annual Growth Rate

DPIF - Data Protection Implementation Framework

EHDS - European Health Data Space

EHR - Electronic Health Record

EU - European Union

FHIR - Fast Healthcare Interoperability Resources

HHS - Health and Human Services

HIPAA - Health Insurance Portability and Accountability Act

HITECH Act - Health Information Technology for Economic and Clinical Health Act

HL7 - Health Level-7

ID - Identity Document

IPC - Information and Privacy Commissioner

IT - Information Technology

NDPR - Nigeria Data Protection Regulation

NEHRS - National Electronic Health Record System

NEHTA - National E-Health Transition Authority

NHA - National Health Act

NHIMS - National Health Information Management System

NPfIT - National Programme for Information Technology

ONC - Office of the National Coordinator for Health Information Technology

PCEHR Act - Personally Controlled Electronic Health Records Act

PHIPA - Personal Health Information Protection Act

UK - United Kingdom

USD - United States Dollar

Table of Contents

Executive Summary

Electronic Health Records (EHRs) have witnessed increased use in recent years because they can improve healthcare service quality and enable more efficient time use - information on events that impact patient care, such as safety and treatment options, can be assessed more quickly.[1] Importantly, these records make data available for research purposes in a cost effective and time-efficient manner especially because less time is spent recruiting trial subjects and collecting data.

Despite its benefit, Electronic Health Records is faced with security, data protection and interoperability issues. Security is one of Electronic Health Records' major challenges as health records are a goldmine for cybercriminals. In 2018, Singapore suffered a serious data breach which compromised the personal data of 1.5 million SingHealth patients, including that of its Prime Minister Lee Hsien Loong. In addition, outpatient medical data of some 160,000 patients were compromised. The stolen data included patients' names, national identification numbers, addresses, gender, race, and date of birth which are valuable to cyber criminals for sale on the dark web.[2] In Finnish, a hacker gained access to patients' (some of which were underage) medical records from therapy sessions in the Vastaamo psychotherapy centre and began emailing more than 40,000 patients whose data was stolen, threatening to leak them to the internet unless the patients provided payment in bitcoin.[3] Asides from security, there are attendant data protection and interoperability challenges that Electronic Health Records faces.

As a result, safeguards have been made available in policies and legal frameworks to protect health records.

In brief, these are some of the findings from the Paper:

- One of the leading security threats to EHR systems is malicious codes like malware and ransomware. The ransomware incidents regarding EHR data continue to rise, with 2,474 incidents reported in 2020.
- EHRs are also threatened by phishing attacks through emails. According to the United States Federal Bureau of Investigation (FBI), it is the most common crime type, with 241 thousand victims recorded in 2020 alone.
- EHR systems face cloud threats arising from placing data on third-party servers which use little or no encryption.
- There is a lack of trust in the system to keep data safe or ensure that data is accessed by only authorised individuals, affecting people's willingness to consent to data collection.
- Interoperability requires standardised and coded data and allows for collaborative research, large-scale analytics, and sharing of sophisticated tools and methodologies.

At the end of the Paper, the following recommendations were made:

- Ensuring that only authorised individuals have access to information on an EHR system.
- Encryption of data and using two-factor and multi-factor authentication ensure minimal data leaks.
- Entrenching the principle of data protection by design and default.
- Create standards for interoperability applicable to health records.
- Establish a framework for transparency, data sharing and accountability.
- Develop policies to guide researchers in maintaining patient privacy while using health information.
- Training of Health researchers on cybersecurity best practices.

Introduction

The adoption of technology in various sectors has enabled tremendous improvements in economies. Like most sectors, digitalisation in the healthcare industry has the potential to transform medical research. An important pillar of this transformation is implementing electronic health records (EHRs) systems.

In 2021, the size of the Global Electronic Health Records market was USD 24.83 Billion and has been projected set to grow at a robust Compound Annual Growth Rate (CAGR) of 9.3% during the 2022-2028 periods, reaching a total of USD 52.98 Billion by 2027.[4,5] EHR is witnessing widespread adoption in various countries. This surge in its usage provides increased opportunities to improve our understanding of healthcare through research using the data that the system provides.

EHR data has immense benefits, especially for research purposes. This paper examines some of the gaps that EHRs can fill for medical research, challenges fraught with its use for research, the safeguards that have been put in place under policies and legal frameworks to protect data, and concludes by proffering recommendations.

Benefits of Electronic Health Records

Electronic health records are digital mediums that collect and store patient health history, from medical diagnosis to treatment plans, medications, and test results.[6] The overriding reason for the introduction of EHRs is to enable health care providers to have all of the vital health information about a patient at their fingertips and enable its accessibility at the point of care.[7]

Electronically stored health information provides improved and coordinated healthcare service by facilitating quick access to patient records.[8] There is also an increase in the efficiency and productivity of healthcare providers[9] by reducing the amount of time spent on paper documentation. The benefit is that healthcare providers can focus on treating and attending to the needs of patients rather than keeping track of patients' records. Thus, EHRs make available adequate resources for healthcare providers to make sound decisions and evidence-based recommendations about a patient's health.

Further, because EHRs enable health information management electronically, other healthcare providers and researchers can share and easily access patient data irrespective of distance and location. Healthcare providers can obtain up to date information about patients in real-time. Even when a patient changes a healthcare provider, a detailed account of the patient's health record is available for the current healthcare provider to use rather than requiring information from scratch.[10]

Filing the Gaps in Medical Research

Access to patient data for research is necessary for progress in the care delivery,[11] yet it is one of the commonest issues with medical research.[12] The traditional system (paper-based) of storing and recording health information makes data retrieval a challenge for researchers across areas, regions and countries. Electronic health records can combat this resource insufficiency by providing access to robust data sharing systems for large scale, real-time research. The resource necessary for research often takes a significant amount of time, energy and money to collect. Still, efficiency in data collection is achievable with EHR because researchers can easily and quickly draw from already available data.[13] Available data provide an invaluable potential to accelerate knowledge discovery by supporting medical research.[14]

Electronic health records offer a solution to the segregation of health records that plagues the paper-based system. In addition, EHR offers integrations with other electronic systems that enable public health researchers to use medical data to produce research beneficial to society.[15] By combining medical data with other sources, public health organisations and researchers can better monitor disease trends and outbreaks and improve surveillance of potential biological threats.[16] For example, combining electronic health records (EHRs) with health data exchange may allow infectious diseases to be detected and responded to early.

Thus, electronic health records provide researchers with the necessary data to conduct life-saving medical studies with the potential to create groundbreaking solutions to health problems. Also, the integration of EHR systems helps researchers easily locate volunteers for medical trials, which is often a time-consuming process. In addition, research registries can leverage EHR by using EHR data to identify and enroll eligible individuals into the research process. Research registries can even rely entirely on EHR data for research purposes.[17]

Interoperability of health records is also made possible with integrated EHR systems as medical devices and technologies can share, explain and provide health data whenever and wherever a patient receives care. Therefore, providing increased transparency, portability, accessibility, and ease of accessing health information.[18] The National Committee on Vital and Health Statistics noted, "Clinically rich information is now more readily available, in a more structured format, and can be electronically exchanged throughout the health and health care continuum. As a result, the information can be better used for quality improvement, public health, and research and can significantly contribute to improvements in health and health care for individuals and populations."19 In addition, interoperability allows for better health outcomes with more accurate information, thereby increasing the ability to conduct research to improve population health. This is because data sharing and access to health information become easier and faster than the traditional means of storing and retrieving files, often cumbersome and time-consuming. Researchers can also effortlessly identify evidence-based best practices by accessing the most current and latest research available.

Challenges in deploying EHR for Research

Despite these benefits of utilising EHRs for research, there are attendant data security, privacy and data protection risks around its use. There are also interoperability issues arising from the data sharing with EHR systems.

Electronic health records are stored and accessed digitally and contain sensitive and confidential personal information of patients, like doctor's notes, prescription information, lab diagnosis, and personal and insurance-related information, which are too risky to be compromised.[20] However, security poses significant barriers to electronic health record systems as they may be susceptible to various security vulnerabilities. These vulnerabilities depend on whether the EHR system is implemented in-house/local servers or cloud-based. In the former, data is stored within the organisation using local servers. In contrast, for the latter, data is stored externally on a third-party cloud vendor service, relies on a third party for support and can be accessed from many/multiple devices.[21] While the cloud-based system has increasingly become the common standard practice, it poses security risks due to third-party servers and the transfer of data back and forth across internet connections.[22]

Health records are considered the holy grail of personal data and valuable to bad actors[23]. They are in high demand by cybercriminals because they contain potentially-valuable health data, including contact information, health insurance ID, Social Security number, and other sensitive financial details.[24] One of the leading security threats to EHR systems is malicious code. They are unwanted files or programs introduced into a user system. Although malware cannot damage the system hardware or network equipment, it can steal, encrypt or delete data, compromise data, change computer functions or take control of them.[25] In addition, it can monitor computer activity without the user's knowledge. As a result, they make data leakages possible, and data can be compromised or manipulated by cybercriminals or hackers.26 Ransomware is malware that locks users out of their computer or system and demands payment for regained access to data, information, and files while holding the data for ransom.[27] The ransomware incidents regarding EHR data continue to rise, with 2,474

incidents reported in 2020.[28] In August 2021, EHR vendor QRS suffered a cyberattack that exposed the health data of nearly 320,000 individuals when hackers accessed its dedicated patient portal server.[29] In September of the same year, Desert Wells, an Arizona based clinic, suffered a ransomware attack that comprised the EHR data of 35,000 patients and rendered them unrecoverable.[30] Similarly, a ransomware attack took place on the IT systems of a Düsseldorf hospital where patient data became inaccessible, and operations had to be postponed. According to the German authorities, this attack may have led to the death of a patient who had to be sent to a different hospital an additional 32 kilometres away, delaying potentially life-saving treatment.[31]

Security threats can also arise from phishing attacks through email to lure the user into clicking a link and revealing login credentials. It is a simple yet highly dangerous cyberattack on EHR security systems.[32] According to the United States Federal Bureau of Investigation (FBI), it is the most common crime type, with 241 thousand victims recorded in 2020 alone.[33] Other security threats that EHR systems face include cloud threats when data is placed on third-party servers that use little or no encryption, making data in transit vulnerable to exploitative attacks, such as Man-in-the-Middle and other exfiltration methods. Data leakages through personnel who have access to the system, either from malicious intent to disclose records or unwitting negligence due to users' insufficient security education and negligence in following security protocols.

Privacy and confidentiality issues surrounding data collection for EHR systems are also a major challenge to its deployment for research purposes. An individual's right to privacy can hinder data collection for research purposes due to the claim of individuals to be left alone from surveillance or interference from other individuals, organisations or the government.[34] While preserving trust is a crucial factor for building a robust EHR system, there is a lack of trust in the system to keep data safe or ensure that data is accessed by only authorised individuals, affecting people's willingness to consent to the collection of their data.[35] There are also concerns around whether data is sufficiently anonymised and the fear that anonymised data can be pieced with other publicly available information and used to de-identify individuals.[36] There are also concerns about the accuracy and reliability of data entered into EHR systems due to improper use of options such as "cut and paste" and the risk for patients and liability for research organisations.[37]

Interoperability is also a barrier facing EHR deployment for research because interoperability extends beyond the ability to exchange information. For EHR systems to be sufficiently interoperable, they must exchange data, but they must also be able to use data. The system needs to work with standardised coded data for this to happen. Data is standardised and coded in a format that allows for collaborative research, large-scale analytics, and sharing of sophisticated tools and methodologies.[38] However, the lack of standardised data is an issue that currently plagues healthcare systems and limits the ability to share data electronically for patient care.[39]

EHR interoperability also faces the obstacle of an absence of close coordination and collaboration of various stakeholders, including patients, providers, software vendors, legislators, and health information technology (IT) professionals. In addition, the health care delivery system continues to have different stakeholders, with data being more of a commodity and competitive advantage than a basis for coordinated care.[40] Also, data must be compatible with all organisations to take full advantage of the benefits of EHRs to serve patients or even for research purposes. When authorised organisations or people receive and send medical records, they must be compatible even though they use diverse systems. This lack of interoperability solutions and standards is a significant obstacle in exchanging healthcare data between multiple stakeholders.

Safeguards in Policies and Legal Frameworks

Policies and legislative frameworks have been introduced to provide necessary privacy and security safeguards that prioritise cyber protection to preserve privacy and ensure the security of health records on electronic health record systems.

United States

The United States establishes a system of EHRs through legislation as the primary mode of regulation. The Health Insurance Portability and Accountability Act Privacy Rule[41] establishes national standards to protect individuals' medical records and other personal health information. The Rule applies only to covered entities such as health plans, healthcare clearinghouses, and healthcare providers.[42] It does not apply to all persons or institutions that collect individually identifiable health information. Researchers are only covered entities if they are also health care providers who electronically transmit health information in connection with any transaction for which Health and Human Services (HHS) has adopted a standard. For example, physicians who conduct clinical studies during a study must comply with the Privacy Rule if they meet the HIPAA definition of a covered entity.[43]

The Rule requires that appropriate safeguards be put in place to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures of such information without patient authorisation. The Rule also gives patients rights over their health information, including the right to examine and obtain a copy of their health records and request corrections. The HIPAA Security Rule[44] also establishes national standards to protect individuals' electronic protected health information. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information.[45] The HIPAA Security Rule requires providers to implement security measures, which help protect patients' privacy by creating the conditions for patient health information to be available but not be improperly used or disclosed.

The three pillars to securing protected health information outlined by HIPAA are administrative, physical and technical. Physical safeguards are one way of preserving confidentiality. This safeguard ensures that only authorised individuals have access to information. The process of controlling and limiting access begins with authorising users.[46] The user's access is based on pre-established, role-based privileges. For example, an EHR system administrator identifies the users, determines what level of information they need, and assigns usernames and passwords. Also, a two-tier approach to authentication, adding a biometrics identifier scan, such as palm, finger, retina, or face recognition, can be included. Since individuals have confidentiality issues towards sharing their health information, privacy and security measures may positively influence their morale to establish an Electronic health record.[47]

Although controlling access to health information is essential, additional technical security measures such as solid privacy and security policies and procedures are essential to securing patient information. Some technical measures that can be put in place to protect data integrity include firewalls, antivirus software, and intrusion detection software. Firewalls can be used to secure the database where electronic health information resides to render hackers unable to enter the system directly to obtain protected health information. Cryptography can also be used to ensure the security of health information on an electronic health record system. For example, encryption can enhance security and confidentiality when exchanging health information.[48] Decryption methods can also ensure the security of EHRs when patients view them. Another cryptography method is the use of passwords and usernames. By utilising passwords and usernames on electronic health record systems, security breaches can be prevented because they will require users to frequently input their passwords into the system. Passwords and usernames can also provide security for healthcare providers because it establishes role-based access controls. However, passwords and usernames should not contain any information like names and dates of birth that can be used to identify or trace an individual.

The HIPAA Security Rule[49] also requires organisations to conduct audit trails. The Rule requires that organisations document information systems activity and have the hardware, software, and procedures to record and examine activity in protected health information systems. Regardless of the type of safeguards put in place, a complete security program must be in place to maintain the integrity of the data, and a system of audit trails must be operational.[50] Audit trails track all EHR system activity, providing evidence of what was viewed, for how long, by whom, and records of all modifications to electronic health records.[51] Alerts are often set on audit trails to flag suspicious or unusual activity, such as reviewing information on a patient one is not treating or attempting to access information one is not authorised to view. However, audit trails do not prevent unintentional access or disclosure of information but can be used as a deterrent to ward off would-be violators.[52]

The United States also has a Health Information Technology for Economic and Clinical Health (HITECH) Act[53] that promotes EHRs. The framework is detailed and seeks to balance the need to have a clear public policy statement of respect for privacy in the doctor-patient relationship while at the same time setting up a mechanism to allow the research community access to enormous volumes of data in EHRs. The Act authorises the National Coordinator for Health Information Technology's (ONC) Office to develop consistent interoperability standards amongst various healthcare systems. In addition, the Act stresses the significance of reporting data breaches and requires health care organisations to watch for breaches of personal health information from both internal and external sources. For example, suppose an entity encounters a data breach in which the information of 500 or more individuals is compromised; the entity must provide specific details of the breach based upon such protocol.[54] Like the HIPAA Security Rule, as part of the meaningful use requirements for EHRs, an organisation must track record actions and generate an audit trail.

Canada

In Canada, regulatory frameworks are available that cater to EHRs. However, personal health information is mainly regulated under provincial Acts, and the protection of EHRs varies across Canada.[55] Québec has an EHR system introduced in 2013, called the Québec Health Record, to securely share patients' information with other healthcare providers. In addition, the province has developed a robust regulatory framework around the system.[56] The Act respecting the sharing of certain health information 2012[57] establishes the right to be informed of and to receive health information concerning oneself held in the health information banks in the clinical domains or that can be released through the Québec Health Record and to request the correction of that information[58] except for their unique user identification number, held in the health information banks in the clinical domains, in the register of refusals or the electronic prescription management system for medication, or that can be released through the Québec Health Record.[59] Section 99 establishes the confidentiality of information contained in a health information bank in a clinical domain, the register of refusals, the electronic prescription management system for medication, the register of users and the register of providers. This section further providers that any person, partnership or body who receives such information must take appropriate security measures to protect it. Section 63 establishes the access authorisation manager to grant necessary access to providers listed under Section 69.[60]

Ontario also has an EHR system and laws regulating it, which received royal assent in 2016.[61] For instance, Ontario's Personal Health Information Protection Act (PHIPA)[62] provides that health information custodians must take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorised use or disclosure and to ensure that the records containing the information are protected against unauthorised copying, modification or disposal.[63] Further, prescribed organisations under the Act must ensure the accuracy and quality of the personal health information accessible through electronic health records by conducting data quality assurance activities on the personal health information it receives from health information custodians.64 Also, they must take reasonable steps to limit the personal health information it receives to that which is reasonably necessary for developing and maintaining the electronic health record. Also, employees or any other person must not access personal health information unless the employee or person acting on behalf of the prescribed organisation agrees to comply with the restrictions that apply to the prescribed organisation. Furthermore, prescribed organisations must protect the

iintegrity, security and confidentiality of the personal health information accessible through the electronic health record. They must also make available to the public a general description of the administrative, technical and physical safeguards in place to protect personal health information that is accessible through the electronic health record against theft, loss and unauthorised collection, use or disclosure, unauthorised copying, modification or disposal.[65]

Additionally, concerns over privacy breaches can be reported to the Information and Privacy Commissioner (IPC) in the form of a complaint, whose office will then investigate the incident and, where appropriate, levy a fine. In 2016, amendments to PHIPA that regulate EHRs were made under Bill 119.[66] These amendments described what it means to 'use' an Electronic Health Record, created a duty for prescribed organisations to develop and maintain an EHR and set out the requirements of the EHR.

United Kingdom

The United Kingdom follows a hybrid model of EHR but does not have a dedicated digital health legislative framework. As a result, the adoption of EHR in the UK has not been through legislative intervention. Instead, National Health Service programmes and plans have provided a gradual introduction and use of EHR for patients. The National Programme for Information Technology (NPfIT) of 2002 by the government aimed to make EHR usage widespread in the UK.[67] The National Health Service is currently using policy interventions like promoting the Interoperability Toolkit in the UK and providing resources like the Fast Healthcare Interoperability Resources to promote EHR standardisation and usage.[68] The Interoperability Toolkit provides standard specifications, frameworks and implementation guides to support interoperability within local organisations and across local health and social care communities.[69] The Fast Healthcare Interoperability Resources (FHIR) provides the global industry standard for passing healthcare data between systems. The Resource Centre aims to make sure that the correct information is available about each patient so that providers can make the right decisions.[70] The FHIR is part of an international family of standards developed by Health Level-7 (HL7).

The FHIR provides a security measure focused on data access methods and leveraging existing security solutions.[71] The FHIR provides that implementation of security measures should ensure that all communications can be encrypted to prevent unauthorised access, no information leaks when errors occur, and complete audit trails can be constructed and used to detect abnormal access patterns. The FHIR privacy measures[72] are sets of considerations required to ensure that individual data are treated according to an individual's Privacy Principles and Privacy-By-Design. In addition, FHIR includes implementation guidance to ensure that individual preferences can be communicated through access managed by the user, consent etc.

European Union

There is no single common EHR system operating across all EU Member States. Instead, some countries have it, and some do not; and those which do often have different EHRs implemented at regional and municipal levels. On May 3, 2022, the European Commission launched the European Health Data Space (EHDS) to improve access to and control by natural persons over their personal electronic health data in healthcare and for secondary uses of EHR data such as research, innovation, policy-making, patient safety, personalised medicine, official statistics or regulatory activities.[73]

One of its core objectives is to set up strict rules for using individual non-identifiable health data for research, innovation, policy-making and regulatory activities.

Under the Proposed Regulation, citizens have control over their health data, share data with health professionals nationally and cross-border, access health data in electronic form immediately and without any cost, add information, rectify errors, restrict access and obtain information on health data use.[74] In addition, researchers are provided with access to large amounts of high-quality data to carry out research, know what data is available, where and its quality, and access data cheaper and more effectively.[75]

The Proposed Regulation provides a long list of electronic data available for secondary use. They include EHRs, electronic health data from medical registries for specific diseases; clinical trials; research cohorts, questionnaires and surveys related to health; electronic health data from biobanks and dedicated databases, insurance status, professional status, education, lifestyle, wellness and behaviour data relevant to health; among others.[76] Although researchers can access these electronic health data, they can only do so for specific purposes listed under Article 34 that benefits individuals and society.

To ensure privacy and security, Article 29 places a duty on market surveillance authority to require a manufacturer of an EHR system, its authorised representative and other relevant economic operators to take all appropriate measures to ensure that the EHR system no longer presents that risk when placed on the market to withdraw the EHR system from the market or to recall it within a reasonable period. This is where an EHR system presents a risk to natural persons' health or safety or other aspects of public interest protection. Also, Health data access bodies can only provide access to electronic health data through a secure processing environment, with technical and organisational measures and security and interoperability requirements.[77]

Due to the sensitivity of electronic health data, the data minimisation principle may be applied to reduce risks to the privacy of natural persons.[78]

Australia

Australia started its EHR journey by setting up a regulatory authority, the National E-Health Transition Authority (NEHTA), in 2005.79 The NEHTA developed specifications, standards and infrastructure and created unique health care identification numbers for all individuals, providers and organisations. The Personally Controlled Electronic Health Records Act (PCEHR Act) in 2012 brought the EHR system within a legal framework.80 In 2016, the PCEHR Act was superseded by the My Health Records Act, 2012.[81] Section 59 of the Act prohibits the unauthorised collection, use and disclosure of health information contained in a healthcare recipient's My Health Record. However, section 61 provides that participants in the My Health Record system are authorised to collect, use and disclose health information included in a registered healthcare recipient's My Health Record if the collection, use or disclosure of the health information is to provide healthcare to the registered health care recipient or by the access controls set by the registered healthcare recipient; or the default access controls specified by the My Health Records Rules or, by the System Operator.

In 2018, the My Health Records Amendment (Strengthening Privacy) Act was introduced across Australia, and privacy for health records was assured through legislative means.[82] The Act provides that the My Health Records (National Application) Rules[83] may make provisions to ensure that the collection, use and disclosure of data or information does not interfere with the privacy of the kind the Commonwealth has international obligations to protect against, including under Article 17 of the International Covenant on Civil and Political Rights.

Brazil

Like most other countries, Brazil has not responded directly to the demands raised by the EHR, nor has the country modified the general medical legislation to the changing nature of the doctor-patient relationship. No specific EHR privacy legislation has been adopted. However, in Brazil, a reasonably high level of technical privacy protection requirements are enforced by Brazilian Federal Law. The law demands that any legally valid electronic document be certified by the Comitê Gestor Infra estrutura de Chaves Públicas, the organisation operating the official Brazilian public infrastructure to ensure authenticity, integrity, and security of information. In addition to these technical measures.84 Brazil's legislative response to privacy in EHRs is found within its constitution, coupled with a few specific rights on privacy in the telecommunications industry, and supported by a general code of medical ethics framework regarding privacy in the doctor-patient relationship.[85]

However, the Brazilian Data Protection Law regards health data as sensitive data,[86]and its processing can be without the data subject's consent for studies by research entities. The law, however, requires that, where possible, personal data must be anonymised.[87] Also, preventive measures should be adopted to prevent damages due to processing, and technical and administrative measures should also be put in place to protect personal data from unauthorised access, accidental or unlawful situations of destruction, loss, alteration, communication or dissemination.[88]

Under Article 13, the law provides that research entities may have access to personal databases when carrying out public health studies. However, the personal databases must be processed exclusively within the entity and strictly for carrying out studies and research. The law requires databases to be kept in a controlled and secure environment with security practices provided in specific regulations, where possible data should be anonymised or pseudonymised and proper ethical standards related to studies and research should be taken into account.

Nigeria

In Nigeria, given the government's plan toward using Electronic health records, the National Health Information Management System (NHIMS) was established in 2007 to track the progress made in all healthcare interventions.[89] The system provides evidence for health sector reforms and helps address constraints in implementing health interventions. It consists of provisions for appropriate infrastructure and establishing mechanisms and procedures for collecting and analysing health data to provide needed information.

To further the cause of implementing EHR in Nigeria, policy documents such as the Medical Code of Ethics, the National Health Policy 2016, the Nigeria National E-Health Policy and the National Health ICT Strategic Framework 2015-2020 have been implemented. Under Section 22, the Code[90] explicitly mandates personal data security against unlawful interception. Also, Section 44 reinforces patient-doctor confidentiality, binding on healthcare professionals delivering service through health platforms. Any information about a patient must be kept confidential. Similarly, the National Health Policy[91] recognises the need for timely, reliable and accurate data to inform policymaking, and evidence-based decisions, strengthen the national e-health system, strengthen coordination mechanisms and platforms for effective collaboration, harmonising the integration of data-collection, strengthen mechanisms to ensure data protection, confidentiality and security, in line with the provisions of the National Health Act 2014, and strengthening mechanisms to ensure accuracy, timeliness, and completeness of health information from the general population and health facilities. The National Health ICT Strategic Framework[92] also provides a Shared Health Record (SHR) to collect and store electronic health information about individual patients in a centralised repository, shared across different healthcare settings.

Under Section 26 of the National Health Act (NHA), 2014[93], all information concerning a person's health status, treatment or stay in a health establishment should be kept confidential. The section provides that health information can only be disclosed upon a court order or any law with the owner's consent in writing and when non-disclosure will pose a severe threat to public health. Section 27 provides the basis for disclosing health records to a third party, where disclosure is for a legitimate purpose within the ordinary course and scope of their duties, and when such access or disclosure is in the user's interest. Section 28 provides consent as the basis for obtaining patients' health records for research, teaching and studying. However, if the research data does not contain any personally identifiable information, consent will not be required. Section 29 places a duty on any person in charge of a healthcare facility to put necessary structures to prevent unauthorised access to patient records and protect such records online and offline.

In Nigeria, given the government's plan toward using Electronic health records, the National Health Information Management System (NHIMS) was established in 2007 to track the progress made in all healthcare interventions.[89] The system provides evidence for health sector reforms and helps address constraints in implementing health interventions. It consists of provisions for appropriate infrastructure and establishing mechanisms and procedures for collecting and analysing health data to provide needed information.

To further the cause of implementing EHR in Nigeria, policy documents such as the Medical Code of Ethics, the National Health Policy 2016, the Nigeria National E-Health Policy and the National Health ICT Strategic Framework 2015-2020 have been implemented. Under Section 22, the Code[90] explicitly mandates personal data security against unlawful interception. Also, Section 44 reinforces patient-doctor confidentiality, binding on healthcare professionals delivering service through health platforms. Any information about a patient must be kept confidential. Similarly, the National Health Policy[91] recognises the need for timely, reliable and accurate data to inform policymaking, and evidence-based decisions, strengthen the national e-health system, strengthen coordination mechanisms and platforms for effective collaboration, harmonising the integration of data-collection, strengthen mechanisms to ensure data protection, confidentiality and security, in line with the provisions of the National Health Act 2014, and strengthening mechanisms to ensure accuracy, timeliness, and completeness of health information from the general population and health facilities. The National Health ICT Strategic Framework[92] also provides a Shared Health Record (SHR) to collect and store electronic health information about individual patients in a centralised repository, shared across different healthcare settings.

Under Section 26 of the National Health Act (NHA), 2014[93], all information concerning a person's health status, treatment or stay in a health establishment should be kept confidential. The section provides that health information can only be disclosed upon a court order or any law with the owner's consent in writing and when non-disclosure will pose a severe threat to public health. Section 27 provides the basis for disclosing health records to a third party, where disclosure is for a legitimate purpose within the ordinary course and scope of their duties, and when such access or disclosure is in the user's interest. Section 28 provides consent as the basis for obtaining patients' health records for research, teaching and studying. However, if the research data does not contain any personally identifiable information, consent will not be required. Section 29 places a duty on any person in charge of a healthcare facility to put necessary structures to prevent unauthorised access to patient records and protect such records online and offline.

In 2019, the National Electronic Health Record System Bill was introduced. The Bill will establish a National Electronic Health Record (NEHR) system that records patients' health information. The aim is to provide electronic health records to enable healthcare professionals, including researchers, to easily access health information. In addition, the Bill currently provides for establishing and maintaining an Index Service where patients' health records can be pooled together.[94] Under Section 13, a registered healthcare recipient can control who may access the recipient's information. The Bill requires that default access controls be placed where such a recipient does not set such controls. Section 14(1) places a penalty on persons who access health records without authorisation.[95] Section 14(1) places a penalty on persons who access health records without authorisation.

Under the Nigeria Data Protection Regulation (NDPR) 2019[96], which is currently the country's general data protection law, health data is considered sensitive personal data requiring a higher degree of protection. The Regulation imposes obligations on data controllers and processors, grants rights to data subjects (patients), and prescribes penalties for non-compliance. The Data Protection Implementation Framework (DPIF) is a supplement to the NDPR, and it offers clarification where the NDPR is silent or unclear. The DPIF makes consent the only lawful basis to process sensitive personal data.[97]

Recommendations

Considering the identified challenges to the use of EHR for research, the following recommendations are put forward:

Privacy and Security

Privacy and security should be made a key component of an EHR system, and this can be maintained by:

- Ensuring that only authorised individuals have access to information on an EHR system. This can be by assigning usernames and passwords, requiring that passwords be changed at set intervals, using a minimum number of characters, and prohibiting the reuse of passwords. Also, a two-tier approach to authentication, such as a biometrics identifier scan of the finger, retina, or face recognition, may be used.

- Access to an EHR system should be based on pre-established, role-based privileges. Users should only have access to the information they need to fulfil their roles and responsibilities, and they must know that they are accountable for the use or misuse of the information they view and change.

- Audit trails should be implemented so that organisations can precisely monitor who has had access to patient information, and alerts should be set to flag suspicious or nusual activity.

- Data should be encrypted to ensure that sensitive data stays secure with minimal chances of data leaks. This means that health information cannot be read or understood except by those using a system that can "decrypt" it with a "key". Also, all associated online traffic should be encrypted. Finally, data encryption should ensure that data is protected as it moves from on-site networks to the cloud or stored and processed in cloud applications.

- A multi-factor authentication, which requires additional measures before access permission is granted, often via another electronic device such as a phone or a tablet, should be implemented to prevent phishing scams. In addition, fingerprint authentication can be employed.

- Healthcare researchers should be trained and educated on cybersecurity best practices and how to deal with emails, websites, suspicious links, and file downloads.

- Researchers should only use messaging and collaboration apps designed for transmitting data that promise to secure data as it traverses the internet and protects it afterwards while it rests in cloud storage.

Policy

Policies and regulatory frameworks for EHR systems should:

- Entrench the principle of data protection by design and default.

- Create standards for interoperability applicable to health records, and quality assurance should be put in place.

- Establish a framework for transparency, data sharing and accountability. The requirement for transparency should make it mandatory that patients understand why they provide the data, how data will be protected and provide quantifiable and explicit benefits for providing data.

- A framework for data sharing, transfer, integration and interoperability standards in healthcare should be established. This is because EHR is integral for carrying out holistic, evidence-based research. As such, there should be an implementation of common data standards for the interoperability of health information.

- There should be an update to and implementation of existing policies and legal framework for electronic health.

- Owing to inadequate data governance measures like keeping track of shared data between researchers, bias in research findings may occur. But by keeping track of data sharing history, researchers can have a more robust overview of the data that has been used in other research, thus reducing the potential for bias.
- The increase in the adoption of EHRs worldwide is an excellent opportunity for all health care providers, researchers, and other stakeholders to collaborate. The concerted effort of this group can ensure that EHRs are used more readily for research.
- Medical research organisations should develop policies to guide researchers in maintaining patient privacy while using health information.

Conclusion

The implementation and development of Electronic Health Records are still fraught with many shortcomings. It is crucial to focus on collaboration between stakeholders, resolving the threats to electronic health records, especially the issues around privacy and security, and standardising interoperability in EHR. The key to optimally employing Electronic health records for research purposes lies in enabling interoperability and ensuring that privacy and security concerns are addressed.

References

1. Kiri, 'Electronic Medical Record Systems: A Pathway to Sustainable Public Health Insurance Schemes in Sub-Saharan Africa' <https://www.npmj.org/article.asp?issn=1117-1936;year=2020;volume=27;issue=1;spage=1;epage=7;aulast=Kiri> accessed 9 April 2021.

2. Yu E, 'Singapore Suffers "most Serious" Data Breach, Affecting 1.5M Healthcare Patients Including Prime Minister' (ZDNet)<https://www.zdnet.com/article/singapore-suffers-most-serious-data-breach-affecting-1-5m-healthcare-patients-including-prime/> accessed 3 May 2022.

3. 'Hacker Seeks to Extort Finnish Mental Health Patients after Data Breach' (POLITICO, 26 October 2020) <https://www.politico.eu/article/cybercriminal-extorts-finnish-therapy-patients-in-shocking-attack-ransomware-blackmail-vastaamo/> accessed 3 May 2022.

4. 'Bloomberg - Are You a Robot?' <https://www.bloomberg.com/tosv2.html?vid=&uuid=97db86b7-cebc-11ec-b0fb-564773566a4e&url=L3ByZXNzLXJlbGVhc2VzLzIwMjItMDUtMDYvYXQtOS0zLWNhZ3ltZ2xvYmFsLWVsZWN0cm9uaWMtaGVhbHRoLXJlY29yZHMtZWhyLW1hcmtldC1zaXplLXRvLWhpdC11c2QtNTItOTgtYmlsbGlvbi1ieS0yMDI3LXNheXMtYnJhbmRlc3NlbmNlLW1hcmtldA==> accessed 8 May 2022.

5. 'EHR Market Value Worldwide 2020-2027' (Statista) <https://www.statista.com/statistics/1264328/ehr-market-value-worldwide/> accessed 8 May 2022.

6. Phaneuf A, 'What Is an EHR System? Definitions, Benefits, Problems and Trends for Electronic Health Records' (Business Insider) <https://www.businessinsider.com/electronic-health-records-benefits-challenges> accessed 3 April 2021.

7. Kruse CS and others, 'Security Techniques for the Electronic Health Records' (2017) 41 Journal of Medical Systems <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5522514/> accessed 3 April 2021.

8. 'What Are the Advantages of Electronic Health Records? | HealthIT.Gov' <https://www.healthit.gov/faq/what-are-advantages-electronic-health-records#:~:text=EHR%20s%20help%20providers%20better,for%20more%20coordinated%2C%20efficient%20care> accessed 3 April 2021.

9. Anonymous, '7 Benefits of Electronic Health Records for Hospitals' (The University of Scranton Online, 20 November 2015) <https://elearning.scranton.edu/resource/health-human-services/7-benefits-electronic-health-records> accessed 4 April 2021.

10. Ibid.

11. Tantoso E and others, 'Hypocrisy Around Medical Patient Data: Issues of Access for Biomedical Research, Data Quality, Usefulness for the Purpose and Omics Data as Game Changer' (2019) 11 Asian Bioethics Review 189 <https://doi.org/10.1007/s41649-019-00085-3> accessed 17 April 2022.

12. Kabiru D. G., & Yahya I. H, "Significance and Challenges of Medical Records: A Systematic Literature Review" Bayero University Kano, Nigeria. ISST Journal of Advances In Librarianship, Vol. 9 No. 1, (January- June 2018), p.p. 26-31 <https://www.researchgate.net/profile/Kabiru-Danladi-Garba/publication/330039863_SIGNIFICANCE_AND_CHALLENGES_OF_MEDICAL_RECORDS_A_SYSTEMATIC_LITERATURE_REVIEW/links/5c2b4718458515a4c70498ca/SIGNIFICANCE-AND-CHALLENGES-OF-MEDICAL-RECORDS-A-SYSTEMATIC-LITERATURE-REVIEW.pdf> accessed 17 April 2022.

13. Institute of Medicine (US) Forum on Drug Discovery, Development. Challenges in Clinical Research. National Academies Press (US), 2010. <https://www.ncbi.nlm.nih.gov/books/NBK50888/> accessed 3 April 2021.

14. Dagliati, Arianna, et al. "Health Informatics and EHR to Support Clinical Research in the COVID-19 Pandemic: An Overview." Briefings in Bioinformatics, vol. 22, no. 2, Mar. 2021, pp. 812–22. Silverchair, doi:10.1093/bib/bbaa418.

15. Aspden P. Patient Safety Achieving a New Standard for Care. Washington, DC: National Academies Press; 2004. <https://www.oliveviewim.org/wp-content/uploads/2018/10/IOM-Patient-Safety.pdf> accessed 4 April 2021.

16. Kukafka R, Ancker JS, Chan C, et al. Redesigning electronic health record systems to support public health. J Biomed Inform. 2007; 40 (4):398–409.

17. Ehrenstein, Vera, et al. Obtaining Data from Electronic Health Records. Agency for Healthcare Research and Quality (US), 2019. <https://www.ncbi.nlm.nih.gov/books/NBK551878/> accessed 4 April 2021.

18. Saini P, 'Why Is EHR Interoperability Important?' (Medium, 6 July 2020) <https://medium.com/@parul.saini.6903/why-is-ehr-interoperability-important-168a7418655f> accessed 4 April 2021.

19. NCVHS (National Committee on Vital and Health Statistics). Enhanced protection for uses of health data: A stewardship framework for "secondary uses" of electronically collected and transmitted health data. 2007a. <http://ncvhs.hhs.gov/071221lt.pdf> accessed 17 April 2022.

20. Halder S, 'Electronic Health Records: Adoption and Overcoming the Challenges for India' <https://www.appknox.com/blog/adoption-of-electronic-health-records-india> accessed 3 April 2021.

21. 'Electronic Health Record Systems' (Office of Information Security 2020) <https://www.hhs.gov/sites /default /files/electronic-health-record-systems.pdf> accessed 19 April 2022.

22. Ibid.

23. 'The Value of Healthcare Data | SecureLink' (30 June 2021) <https://www.securelink.com/blog/healthcare-data-new-prize-hackers/> accessed 2 May 2022.

24. Kassner M, 'How to Keep EHRs Secure and Safe from Cybercriminals' (TechRepublic, 22 July 2018) <https://www.techrepublic.com/article/how-to-keep-ehrs-secure-and-safe-from-cybercriminals/> accessed 19 April 2022.

25. 'Top-5 Cyber Threats to EHR Systems and How to Deal with Them' (Erbis Blog, 26 October 2021) <https://erbis.com/blog/top-5-cyber-threats-to-ehr-systems-and-how-to-deal-with-them/> accessed 19 April 2022.

26. Ibid at 1.

27. Kill G, 'Top 5 Cybersecurity Threats to Electronic Medical Records' (Integracon, 29 April 2018) <https://integracon.com/top-5-cybersecurity-threats-to-electronic-health-records-and-electronic-medical-records/> accessed 19 April 2022.

28. 'Crime Internet Report' (Federal Bureau of Investigation 2020) <https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf> accessed 19 April 2022.

29. McKeon J and, '320K Impacted in EHR Vendor Breach, Ransomware Hits Health Systems' (HealthITSecurity) <https://healthitsecurity.com/news/320k-impacted-in-ehr-vendor-breach-ransomware-hits-health-systems> accessed 19 April 2022.

30. 'Ransomware Attack Wipes out Arizona Clinic's EHR, Corrupts 35,000 Patients' Records ' <https://www.beckershospitalreview.com/cybersecurity/ransomware-attack-wipes-out-arizona-clinic-s-ehr-corrupts-35-000-patients-records.html> accessed 19 April 2022.

31. Moss S. 'Patient dies after German hospital IT systems were hacked' DCD, 18 September 2020) <https://www.datacenterdynamics.com/en/news/patient-dies-after-german-hospital-it-systems-were-hacked/> accessed 3 May 2022.

32. 'Top-5 Cyber Threats to EHR Systems and How to Deal with Them' (Erbis Blog, 26 October 2021) <https://erbis.com/blog/top-5-cyber-threats-to-ehr-systems-and-how-to-deal-with-them/> accessed 19 April 2022

.

33. Ibid at 22.

34. Harman LB, Flite CA and Bond K, 'Electronic Health Records: Privacy, Confidentiality, and Security' (2012) 14 AMA Journal of Ethics 712 <https://journalofethics.ama-assn.org/article/electronic-health-records-privacy-confidentiality-and-security/2012-09> accessed 19 April 2022.

35. Ozair FF and others, 'Ethical Issues in Electronic Health Records: A General Overview' (2015) 6 Perspectives in Clinical Research 73 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4394583/> accessed 19 April 2022.

36. Aselton P and Affenito S G, 'Privacy Issues with the Electronic Medical Record' (Online Qualitative research, 2014) <https://www.researchgate.net/profile/Pamela-Aselton/publication/266741222_Privacy_Issues_with_the_Electronic_Medical_Record/links/5652357e08ae1ef929756917/Privacy-Issues-with-the-Electronic-Medical-Record.pdf> accessed 19 April 2022.

37. Ibid at 28.

38. 'Data Standardisation – OHDSI' <https://www.ohdsi.org/data-standardization/> accessed 3 April 2021.

39. Council for Affordable Quality Healthcare, 'Defining the Provider Data Dilemma: Challenges, Opportunities, and Call for Industry Collaboration' <www.caqh.org/sites/default/files/explorations/defining-provider-data-white-paper.pdf> accessed 7 April 2021.

40. Reisman M, 'EHRs: The Challenge of Making Electronic Data Usable and Interoperable' (2017) 42 Pharmacy and Therapeutics 572.

41. Health Insurance Portability and Accountability Act of 1996 HIPAA Privacy Rule <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html> accessed 8 April 2021.

42. For example, hospitals, academic medical centres, physicians, and other health care providers who electronically transmit claims transaction information directly or through an intermediary to a health plan.

43. 'HIPAA Privacy Rule and Its Impacts on Research' <https://privacyruleandresearch.nih.gov/pr_06.asp#:~:text=The%20Privacy%20Rule%20applies%20only%20to%20covered%20entities%3B%20it%20does,covered%20entities%20to%20provide%20PHI.> accessed 3 May 2022.

44. Health Insurance Portability and Accountability Act of 1996 HIPAA Security Rule <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html> accessed 7 April 2021.

45. The Office of the National Coordinator for Health Information Technology 'Guide to Privacy and Security of Health Information' <https://www.healthit.gov/sites/default/files/pdf/privacy/onc_privacy_and_security_chapter4_v1_022112.pdf> accessed 7 April 2021.

46. 'Security and Privacy of Electronic Health Records: Concerns and Challenges' [2020] Egyptian Informatics Journal <https://www.sciencedirect.com/science/article/pii/S1110866520301365> accessed 9 April 2021.

47. Harman LB, Flite CA and Bond K, 'Electronic Health Records: Privacy, Confidentiality, and Security' (2012) 14 AMA Journal of Ethics 712 < https://journalofethics.ama-assn.org/article/electronic-health-records-privacy-confidentiality-and-security/2012-09> accessed 7 April 2021.

48. Ibid.

49. Health Insurance Portability and Accountability Act of 1996 HIPAA Security Rule <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html> accessed 9 April 2021.

50. Ibid at 22.

51. American Health Information Management Association. <http://library.ahima.org/29%3Cand%3E%28xPublishSite%3Csubstring%3E%60BoK%60%29&SortField=xPubDate&SortOrder=Desc&dDocName=bok1_042564&HighlightType=PdfHighlight> accessed 8 April 2021.

52. Ibid at 12.

53. 2009.<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf> accessed 8 April 2021.

54. Wikina SB. What caused the breach? an examination of the use of information technology and health data breaches. Perspect. Health Inf. Mana. 2014;2014:1–16.

55. Team AM| R, 'Electronic Health Records: A Glimpse into the Legal Framework' (McGill Journal of Law and Health, 15 February 2019) <https://mjlh.mcgill.ca/2019/02/15/electronic-health-records-a-glimpse-into- the-legal-framework/> accessed 19 April 2022.

56. Legal and Regulatory Framework - Québec Health Record <https://www.quebec.ca/en/health/your-health-information/quebec-health-record/legal-and-regulatory-framework/> accessed 9 April 2021.

57. '- Act Respecting the Sharing of Certain Health Information' <https://www.legisquebec.gouv.qc.ca/en/document/cs/P-9.0001> accessed 19 April 2022.

58. Section 9(3).

59. Section 112. This provision exempts a minor under the age of 14.

60. See the additional category of providers under the Regulation respecting the application of the Act respecting the sharing of certain health information. https://www.legisquebec.gouv.qc.ca/en/document/cr/P-9.0001,%20r.%200.1.

61. Team, Author MJLH |. RDSM. "Electronic Health Records: A Glimpse Into the Legal Framework." McGill Journal of Law and Health, 15 Feb. 2019, <https://mjlh.mcgill.ca/2019/02/15/electronic-health-records-a-glimpse-into-the-legal-framework/> accessed 9 April 2021.

62. 2004, c. 3. A "Law Document English View." Ontario.Ca, 24 July 2014, <https://www.ontario.ca/laws/view> accessed 15 April 2021.

63. Section 12(1).

64. Section 55(2).

65. Section 55(3).

66. "Health Information Protection Act, 2016." Legislative Assembly of Ontario, <https://www.ola.org/en/legislative-business/bills/parliament-41/session-1/bill-119> accessed 13 April 2021.

67. O Campion-Awwad, A Hayton, L Smith and M Vuaran, 'The National Programme for IT in the NHS: A Case History' (02/2014) <https://www.cl.cam.ac.uk/~rja14/Papers/npfit-mpp-2014-case-history.pdf> accessed 14 April 2021.

68. Kaur 2020, 'Electronic health records in India: Legal framework and regulatory issues', RGNUL Student Research Review (RSSR), Volume 6, Issue 1 <http://rsrr.in/wp-content/uploads/2020/08/ELECTRONIC-HEALTH-RECORDS-IN-INDIA.pdf> accessed 15 April 2021

69.<https://developer.nhs.uk/wp-content/uploads/2013/03/ITK-Overview-Pack-for-initial-workshop.pdf> Accessed 13 May 2021.

70. "Fast Healthcare Interoperability Resources." NHS Digital, <https://digital.nhs.uk/services/fhir-apis> accessed 12 May 2021.

71. Secpriv-Module - FHIR v4.0.1. <https://www.hl7.org/fhir/secpriv-module.html> accessed 12 May 2021.

72. Ibid.

73. Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197> accessed 4 May 2022.

74. Article 38.

75. Article 55.

76. Article 33.

77. Article 50.

78. Preamble 49.

79. S J Hambleton and J Aloizos AM, 'Australia's digital health journey' <https://www.mja.com.au/journal/2019/210/6/australias-digital-health-journey#12> accessed 13 April 2021.

80. Personally Controlled Electronic Health Records Act 2012. (Australia), <https://www.legislation.gov.au/Details/C2012A00063> accessed 15 April 2021.

81. My Health Records Act 2012 (Australia), <https://www.legislation.gov.au/Series/C2012A00063> accessed 12 April 2021.

82. My Health Records Amendment (Strengthening Privacy) Act 2018 (Australia), <https://www.legislation.gov.au/Details/C2018A00154> accessed 16 May 2021.

83. 2017, <https://www.legislation.gov.au/Details/F2017L01558 > accessed 15 April 2021.

84. World Health Organization, 'Legal frameworks for eHealth' Global Observatory for eHealth series - Volume 5 <https://www.who.int/goe/publications/legal_framework_web.pdf> accessed 13 April 2021.

85. Code of Medical Ethics, Brazil | Encyclopedia.Com. <https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/code-medical-ethics-brazil> accessed 15 May 2021.

86. Brazilian Data Protection Law (LGPD) (As amended by Law No. 13,853/2019) <https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf> accessed 3 May 2022. See Article 5(ii).

87. Article 11(c).

88. Article 6(viii) &(vii).

89. 'NHMIS Monthly Analysis' <https://monthly-nhmis-analysis.fmohconnect.gov.ng/> accessed 9 April 2021.

90. Medical and Dental Practitioners Act [CAP 221], Laws of the Federal Republic of Nigeria 1990. <http://www.mdcnigeria.org/Downloads/CODE%20OF%20CONDUCTS.pdf> accessed 31 March 2021.

91. 2016, <https://naca.gov.ng/wp-content/uploads/2019/10/National-Health-Policy-Final-copy.pdf> accessed 16 May 2021.

92. 2015-2020, < https://www.who.int/goe/policies/Nigeria_health.pdf?ua=1> accessed 13 April 2021.

93. 'No 145 of 2014' <https://nigeriahealthwatch.com/wp-content/uploads/bsk-pdf-manager/2018/07/01_-Official-Gazette-of-the-National-Health-Act-FGN.pdf> accessed 31 March 2021.

94. Section 8(a) of the National Electronic Health Record Bill, 2019 < https://placbillstrack.org/ upload/HB447.pdf> accessed 13 April 2021.

95. A fine not exceeding one million naira and an imprisonment term not exceeding two years for unauthorised disclosure of record. A breach of any provision of the Bill attracts a fine not exceeding one million naira and a term of imprisonment not exceeding two years. A corporation will be subject to a fine not exceeding ten million naira for a breach of the Bill.

96. Nigeria Data Protection Regulation 2019 https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf accessed 31 March 2021.

97. Article 5.3.1 (b) of NDPR. Other legal frameworks that regulate EHR in Nigeria include the 1999 Constitution of the Federal Republic of Nigeria and the Cybercrimes (Prevention and Prohibition etc.) Act 2015.


TECH HIVE
ADVISORY


IKIGAI