Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 3, pp: (58-66), Month: September - December 2023, Available at: www.noveltyjournals.com

Regulations for Securing Patient Data

Sherryl W. Johnson (PhD)[1]

[1]School of Business, Management: Healthcare Administration Program

[1]Albany State University, Albany, Georgia, United States of America

DOI: https://doi.org/10.5281/zenodo.10401160

Published Date: 18-December-2023

Abstract: **With the rapid evolution of health information technology, there is a heightened need for the incorporation of regulations for securing patient data. This is true since the evolution from paper health records to electronic health records and other electronic health information. Accordingly, this scholarly literature view will provide an overview of governmental regulations that have been enacted to protect and secure patient data in the United States of America. International and organizational patient data and security measures and strategies will also be included – along with other strategies to secure patient data from professional organizations, educators and established companies / corporations.**

Keywords: **electronic records, government regulations, health information, information security, patient data.**

I. INTRODUCTION/GOVERNMENTAL REGULATIONS TO PROTECT AND SECURE PATIENT DATA

A. Growth in Data / Electronic Health Records

This paper will review governmental regulations and organizational efforts to secure and protect patient data using current scholarly literature. The expansion of health information in many forms has given rise to the need for regulations to secure and protect patient information. The current era has been elevated by cloud computing, big data and the Internet of Things (IoT) that have led to great challenges in data security and privacy.[1] (Jin et al. 2019). Jin et al., 2019, further reported that electronic medical record (EMR) data, especially protected health information (PHI) suffers from great risk of data breach events – with such breaches happening at a rate of more than one per day.[1]

Thapa and Camtepe, 2021, reported how precision health leverages information from various sources in medical records, medical insurance claims, electronic health monitoring devices, health data centers and more.[2] Thapa and Camtepe, 2021, further reported that security and privacy of patient health data or information is a mandatory requirement for health databases, including personal information worldwide, due to legal provisions, financial reasons and trust. Also, leakage of such private information can affect one's personal life, insurance premiums, job, and security.[2] According to Thape and Camtepe, 2021, governmental legislation and ethics committees require security and privacy of patient data.

B. HIPAA Enactment to Provide Federal Protection of Patients' Health Data

Liberty University, 2021, provides highlights of an important governmental security rule for patient data – the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA is known to healthcare consumers as the privacy law.[3]

The rules of HIPAA apply to all covered entities that electronically process, store, transmit or receive medical records or remittance advices.

A covered entity is a physician, hospital, or health care facility, health insurance company, clearinghouse and business associate of a covered entity that has access to individually identifiable health information.[3] The Security Rule of HIPAA

directly addresses the electronic system used to house, maintain and transmit health information. The rule includes ways to protect electronic health information – and addresses how personal health information is stored, accessed, transmitted and audited.[3]

Duggineni, 2023, stated that ensuring data integrity and security is crucial for the success and reputation of any organization. Data breaches can have serious consequences, including financial losses, damage to reputation, and legal liabilities.[4] Duggineni, 2023, reiterated the fact that the United States Health Insurance Portability and Accountability Act (HIPAA) provides several protections for patient's health data against misuse or exposure and requires technical and administrative controls to ensure compliance.[4] Concoranu et al., 2013 also reported on United States HIPAA security requirements for laboratories.[5]

Hathaliya and Tanwar, 2020, reported that healthcare industries have defined some policies and regulations to access healthcare data – including HIPAA. The authors noted that HIPAA has improved the nation's healthcare system and mandates it for all healthcare organizations to secure health information.[6] Rao et al., 2015 reported in the healthcare sector, the privacy of big data is a major concern and bound by international regulations like HIPAA.[7] Flaumenhaft and Ben-Assuli, 2018 cited HIPAA as the relevant legislation pertaining to personal health records – although noting that the current policy and regulatory framework concerning personal health record services may be fragmented.[8]

According to Andriole, 2014, HIPAA was enacted to serve two main purposes: (1) to protect health insurance coverage for workers and their families when they change or lose their jobs (Title I) and (2) to require the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers (Title II). The Administrative Simplification Statute and Rules (Title II of HIPAA) also addressed security and privacy of health data.[9]

C. The Health Information Technology Economic and Clinical Act and Patient Data Security

The Health Information Technology Economic and Clinical Act (HITECH) another federally enacted mandate regarding health records, required that all health care systems and organizations secure (patient) health information – with increasing emphasis on the extended ranges of health information and cloud technology. With emphasis on regulation, Hathaliya and Tanwar, 2020, presented information on how the health care industry has revolutionized from 1.0 to 4.0 (1.0 – doctor-centric; 2.0 – replacement of manual records with electronic records (EHRs); 3.0 – patient-centric and 4.0 cloud computing, fog computing, Internet of Things (IoT) and telehealthcare) with technologies that share data with various stakeholders.[6]

According to the authors, Healthcare 4.0 may lead to the breach of healthcare records where hackers can gain full access to patients' email accounts, messages and reports. Also, as medical records have transformed into digital records (stored in electronic health records), with accessibility online through the cloud server, servers can be breached giving unauthorized access to patient's medical data.[6] In addition, security for such areas as Healthcare 4.0 – telemedicine needs to be addressed.

According to Andriole, 2014, the HITECH Act was intended to foster interoperable information technology (IT) systems for provider decision-making and high-quality nonredundant care.[9] With the act came healthcare exchanges and personal health records – which increase opportunities for inappropriate exposure to health information. Safeguards are needed to maintain privacy and confidentiality of health information.[9] Cucoranu et al., 2013 provided an overview of the HITECH Act reflecting on its being signed into law on February 17, 2009.[5] According to the authors, the Security Breach Notification Rule within the HITECH Act requires covered entities and their business associates to notify any affected patient when the security of their personal health information has been compromised, in no case later than 60 days following the breach discovery.[5]

Cucoranu et al., 2013 further explained that covered entities must notify the Secretary of the Department of Health and Human Services and the media outlets when a breach affects more than five hundred people.[5] According to Cucoranu et al., 2013, HITECH also imposes significant penalties for unauthorized disclosures - ranging from fines to possible imprisonment.[5] Flaumenhaft and Ben-Assauli, 2018, also identified the HITECH Act of 2009 as pertinent to personal health record security and privacy regulation.[8]

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 3, pp: (58-66), Month: September - December 2023, Available at: www.noveltyjournals.com

D. HIPAA and HITECH Extend Security and Privacy of Health Information to Business Associates

Jin et al., 2019, reported that both HIPAA and the HITECH Act extend security and privacy requirements to business associates – with guidelines for keeping patient data secure whenever it is accessed, saved, shared. The authors included HIPAA technical safeguard requirements – including access control, audit controls, integrity, person / entity authentication and transmission security.[1]

E. The American Recovery and Reinvestment Act of 2009 and Patient Data Security

The American Recovery and Reinvestment Act of 2009 was used to reinforce HIPAA for privacy and security and breach notification of health records of all United States citizens.[10] Liberty University, 2021, further highlighted the changes of 2009 with the passage of the Affordable Care Act (ACA) and the American Recovery and Reinvestment Act, which included the Health Information Technology for Economic and Clinical Health Act – HITECH.[3]

F. The United States Food and Drug Administration and Patient Data Security

Another way the United States has moved to meet regulatory expectations for data integrity is through the United States Food and Drug Administration. To assure data integrity in the pharmaceutical industry parts of 21 code of Federal Regulations have been enforced. Specifically, 21 CFR Part 11 which went into effect in 1997 extended data integrity regulations related to electronic records and electronic signatures.[4] In the age of data breaches, it is increasingly important that data security measures be implemented to secure data. According to Cucoranu et al., 2013, in 2005 the Federal Drug Administration issued a notice that Cybersecurity for Networked Medical Devices was a shared responsibility. However, the authors reported that new regulations related to secure authentication, tracking for mobile devices and use of clinical software were still needed.[5]

Further 45 CFR Code of the Federal Regulations Section 164.514 stated that accession numbers that are designed to uniquely identify a patient within a health facility, should be treated as personal health information. Legal requirements for identifying protected health information includes name, address, zip code, birth date, admission date, discharge date, date of death, telephone number, fax number, electronic mail address, social security number, medical records number and more. [5]

G. The Federal Trade Commission and Patient Data Security

Rao et al., 2015 reported that in the healthcare sector, the privacy and security of data is bound by the Federal Trade Commission – especially in relation to international regulation.[7] According to Sayeed et al., 2021,

Under the 21st Century Cures Act and the Office of the National Coordinator for Health Information Technology (ONC) rule implementing its interoperability provisions, a patient's rights to easily request and obtain digital access to portion of their medical record are new supported by both technology and policy. Data, once directed by a patient to leave a Health Insurance Portability and Accountability Act – covered health entity and enter a consumer app, will fall under Federal Trade Commission oversight.[11]

H. The United States Department of Health and Human Services and Patient Data Security

The Department of Health and Human Services published a final Privacy Rule in December (modified in August 2002) that set standards for the protection of individually identifiable health information.[9] It also published the Security Rule in February 2003 that set standards for confidentiality, integrity, and availability of electronic protected health information.[9]

The HIPAA Privacy Rule (2000) gave patients certain rights over their health information (the ability to obtain a copy of their health record) meanwhile protecting the privacy of personal health information.[5] In 2002, the privacy rule was updated to establish national standards for the protection of health information including unique health identifiers and electronic transmission and signature authentication.[5]

II. INTERNATIONAL PATIENT HEALTH INFORMATION POLICIES AND SECURITY REGULATIONS

A The need for securing and protecting patient information is not only a national phenomenon. International policies for patient data protection and security includes various countries and continents such as Sweden, China, the United Kingdom, Europe and Australia.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 3, pp: (58-66), Month: September - December 2023, Available at: www.noveltyjournals.com

A. Swedish Initiatives on Patient Data Security

According to Agrawal and Prabakan, 2020, Sweden uses national identification numbers as a method of linking clinical and administrative data sets. Sweden has also established a cancer registry for patient information.[12] Specifically, the Swedish government has committed over $70 million dollars annually to expand a variety of cancer registries that would allow researchers to determine the risk factors for cancer. Each patient's entries are linked to unique identity numbers that can be cross references with other ninety other registries to give more complete patient's information based on health and other circumstances.[12] The idea of unique patient identifiers is a novel approach to big data initiatives, health research and patient health information security.

B. Chinese Initiatives on Patient Data Security

China has leveraged unique identify numbers for citizens to link disconnected data sets – and has established a cancer registry for patient information.[12] According to Zhang et al., 2018, the central government of China has started several funding initiatives aimed at integrating Big Data into health care cases – linking administrative data, regional claims data from national health insurance programs, and claims data from electronic medical records.[13]

C. The United Kingdom and Patient Data Security

The United Kingdom has centralization and regulations related to the use of health care data – and example being the United Kingdom Biobank.[12] Specifically, the United Kingdom is broadly leveraging the centralization of the National Health Service to link genomic data with clinical care records and opening up the disease endpoints to researchers through a patient ID.[12] The United Kingdom has been heralded for its National Health Service's ability to successfully integrate a variety of health records.[12] Also, the United Kingdom has begun the process of digitizing its health services, with separate National Health Services Trusts adopting American electronic health record solutions.[14] With the efforts to link patients through a patient ID and advanced digitation, privacy, security and efficient use of data will continue to be concerns in the United Kingdom.

D. European Efforts to Provide Patient Data Regulation and Security

In the European Union's General Data Protection Regulation, personal information is defined as any data that relates to an identified or identifiable individual.[2] Such data includes online identifiers, location information, bio-metric data, and health information. Jin et al., 2019 further reported that the General Data Protection Regulation in Europe requires data to be stored and shared in a secure and privacy-preserving way and individuals may incur severe penalties for events of a healthcare data breach.[1]

E. Australian Efforts to Provide Patient Data Regulation and Security

Based on the Privacy Act of 1988, Australia has defined personal information as information that identifies an individual and includes information about an individual's health.[2] Based on a patient engagement survey in 2018 by Medical Direction partnership with HotDoc, it was found that 91% and 93% of Australians rated health information data security and privacy as a major concern, respectively.[2] The authors also reported that among all data breaches health data covers a major portion.[2]

Swede et al., 2019 reported that globally theft of healthcare records counts among the costliest in the industry.[10] It was estimated that the average cost of a stolen record was $382, according to the 2017 Cost of a Data Breach Study: Global Overview by the Ponemon Institute and IBM, up from $355 in 2016.[15] Such a finding highlights the global needs for measures to secure and protect patient data.

III. ORGANIZATIONAL MEASURES TO SECURE PATIENT DATA

With the use of electronic medical records and the increase in the use of electronic transfer of data, the protection of patient records has become a critical issue for health providers,[10] health organizations and other organizations housing patient data. Duggineni, 2023 reported 5212 companies across the globe with data breaches from November 2020 to October 2021, health care organizations ranked second with 571 data breaches – while finance organizations ranked first with 690.[4]

While human error drives many security breaches, Swede et al., 2019 suggested that security practitioners should be aware of the many roles human and organizational factors play in security breaches.[10] Swede et al., 2019 further reported that the definition of information security to maintain security within a computer system has been broadened to include both technical and non-technical activities.[10]

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 3, pp: (58-66), Month: September - December 2023, Available at: www.noveltyjournals.com

A. HIPAA and HITECH Technical Safeguards for Health Information

Jin et al., 2019 reported that HIPAA and HITECH require organizations to apply technical safeguards for health information - besides the confidentiality, integrity and authentication (identify confirmation) requirement.[1] Access control with identify tracking and emergency access, and activity auditing are also included.

Cucoranu et al., 2013, added that HIPAA policies and procedures include Administrative Safeguards including security management functions, assigned security responsibility, workforce security, information access management, security awareness training, security incident procedures, contingency plan and evaluation. Physical Safeguards include facility access control, workstation use, workstation security, device and media controls, and endpoint security. Technical Safeguards including access control, audit control, integrity, person or entity authentication and transmission security.[5]

B. Access Control / Cards As Organizational Measure to Support Data Security

Duggineni, 2023, reported on highly impactful robust measures to ensure the integrity and security of data throughout its lifecycle. By implementing access control – meaning data access permissions should be strictly controlled to individuals with the necessary authorization. It was noted that access should only be given to individuals that require it and adhere to a least privileged model of security.[4]

Cucoranu et al., 2013 also included access control as a potential threat topic related to security breaches (protection against malicious intrusion or data theft, and recovery from security breaches and privacy.[5] Information systems should have the ability to control which users can access the system – and what information they can view.[5] The author further suggested that facility access control to areas where servers, terminals and modems are stored be limited to individuals with access cards. Also, the areas should be kept locked at all times.[5]

C. Audit Trails Use to Protect Patient Data

Audit trails also play a vital role in security and protection of patient data. According to Cucoranu et al., 2013 modern information systems have the capabilities to perform additional (random and by request) audits on access, record viewing and modification of patient data.[5] Duggineni 2023 stated that automatic audit monitoring systems are useful in identifying the origin of data changes.[4] In the event of a data breach, the audit trail should be helpful in identifying the breach's origin and tract data events like creation, deletion, updating - in addition to the exact time of the function originated.[4]

D. Backing Up Data Can Aid in Data Security

Cucoranu et al., 2013 described data backup as a measure to secure and protect patient data. Backup was defined as the process of copying and archiving computer data that can be used to restore the original after a data loss event.[5] Liberty University, 2021, indicated that servers housing patient records must be backed up whether to prevent data loss from a natural disaster or a technical failure.[3] The author further highlighted the need for parallel backup systems to circumvent cyberattacks and data breaches.[3]

Duggineni, 2023, reiterated that backing up data makes sure that no data is lost in the event of a data loss. Accordingly, it is important that timely and regular back up features have controlled access to limited users.[4] Cucoranu et al., 2013 reported that unplanned outages that can result in data loss can be prevented by type of back up (periodic vs. real-time), location of backups (onsite, off-site or both), backup media (such as storage area network technology) and appropriate personnel to perform disaster recovery (internal or external).[5] Cucoranu et al., 2013 further reported that continuous back up can restore data at any given time.[5]

E. Vetting and Preparing Personnel is a Measure to Secure Organizational Data

Rizvi et al., 2020 provided insight on patient data security and privacy – especially in the age of the Internet of Things (IoT).[16] The authors stated that personal data remains vulnerable due to the unregulated nature of the IoT devices.[16] Rizvi et al., 2020, suggested that to minimize data breaches, proper personnel must be thoroughly vetted and prepared for securing organizational and customer data.[16] Cucoranu et al., 2013 stated that responsibility for security implementation and compliance is the responsibility of the healthcare entity that manages the data.[5] With the advent of home health monitoring devices, the scope of health-care entities increases.

F. Security Risk Analysis Can Be Used to Secure Patient Data

According to Cucoranu et al., 2013, a security risk analysis is a systematic process designed to examine and identify any potential threats and vulnerabilities – with monitoring of changes. The identified risks may be addressed through policy, training and new technology.[5]

G. Passwords To Secure Electronic Patient Data

Andriole, 2014 included log-ins / usernames and passwords as tools to maintain security and privacy of patient health information.[9] Cucoranu et al., 2013 addressed the use of passwords as a security measure in the pathology laboratory.[5] Additionally, the authors included the concept of password aging – the process of forcing users to change access passwords with a specific frequency (password expiration). Passwords can be enhanced with mixed letter casing, numbers, encryption, timed changes and more.[5] Other privacy, protection and security measures that were presented by the authors include data encryption, antiviral software, firewalls and authentication.[5]

H. Data Encryption As a Security Measure for Patient Data

Data encryption is the process of changing readable text into a set of characters and numbers based on mathematical algorithms.[5] Jin et al., 2019 reported that single administrative domains are insufficient for medical data sharing across multiple health domains.[1] Thus, the authors suggested that more advanced cryptographic primitives with rich access control semantics and strict confidentiality enforcement be required.[1]

I. Anti-viral Software to Protect Patient Data

Anti-viral software is used to prevent, detect and remove malware.[5] Kruse et al., 2017, stated that according to the cyber-security checklist created by the Office of the National Coordinator for Health Information Technology, antivirus software is in the top ten listed methods for avoiding security breach.[17]

J. Firewalls to Protect Patient Data

Liberty University, 2021, reported that firewalls prevent unauthorized access into or out of the network and the use of both hardware and software devices that filter activity over the network.[3] Cucoranu et al., reported that most healthcare providers and hospitals choose to build their health care system in a closed domain with a defensive perimeter, such as a private network equipped with firewalls and intrusion detection systems. [5] According to the authors, while firewalls add an additional layer of protection for health care data, the firewalls create medical data silos[5] – unlike cloud computing and big data that support data sharing.[1]

K. Authentication Can Be Used To Protect Patient Data

Kruse et al., 2017 presented authentication among the measures to secure patient data.[17] According to Cucoranu et al., 2013 authentication is useful in patient data security In the United States, the National Institute of Standards Technology (NIST) issued an electronic authentication guideline with multi-levels of assurance for the authentication process.[5] Various authentication techniques included user-name – password pairs, single-sign on, biometrics, and hardware or software tokens.[5]

IV. EDUCATIONAL, PROFESSIONAL SOCIETIES AND CORPORATE STRATEGIES TO SECURE PATIENT DATA

In addition to patient data security measures utilized in healthcare organizations, other strategies have been proposed by educators, professional societies and corporations / companies. Som of the strategies are as follows:

A. Health Science and Computer Science Professionals Propose a Curriculum for Patient Data Protections

Swede et al., 2019 reported that health science and computer science professionals proposed a curriculum to help health care students understand and comply with governmental and institutional policies on patient data protection during clinical rotations or during annual employee trainings.[10] The authors stated that such training regarding sharing, transmission, storage and access of patient health information is necessary to prevent breaches of health care information. The training should extend beyond HIPAA and focus on specific rules and regulations of the organization.[10] Suggested modules for

training included Cyberspace Laws and Regulations Applicable to Healthcare; Defining the Internet in Terms of Cloud Computing; How IT Departments Secure Patient Data; Appreciation of the Role of Health Information Management Professionals, and Development of a Cybersecurity Plan. In essence, the final module would ask the student to create a best practices cybersecurity plan to guide employees.[10]

B. Professional Organizations Collaborate to Protect Patient Data

Additionally, professional organizations such as the American College of Radiology, Radiology Society of North America, and the Society of Imaging in Informatics in Medicine have worked collaboratively to publish a document on securing identifiable patient information - including images.[9] The guidance considers standards, policies, procedures, technologies, educational modalities and other information regarding providing high quality medical care in a safe and secure environment. [9] The author also cited the role of the HIPAA and HITECH Act in data security information exchanges and interoperability – along with ways to limit appropriate exposure.[9]

C. Health Level Seven (HL7) Adopted Techniques to Promote Patient Data Security

Health Level Seven (HL7) is an international standards body focused on the exchange, integration, sharing and retrieval of electronic health information that supports clinical practice and management. HL7 programming is critical to interfaces between systems to allow interoperability. HL7 is an exchange format.[3] Agrawal and Prabakaran, 2020, reported that HL7 had published a new standard for healthcare data exchange called Fast Healthcare Interoperability Resources (FAIT).[12] Cucoranu et al., 2021 reported that the single sign-on, endorsed by HL7, enables users to use one ID and password pair to access multiple related, but independent systems.[5] In relation to reducing password fatigue, single sign-on also reduces information technology costs. Even so, synchronization errors may result causing patient harm – and limiting patient data protection and security.[5]

D. Big Data – Machine Learning Integration with the Electronic Health Record Enhancing Patient Data Transfer / Security

In relation to patient data security and protections, Agrawal and Parabakan, 2020, reported that effective use of Big Data in healthcare has been enabled by the development of machine learning approaches.[12] Application of machine learning (ML) tools is also supplemented by the widespread adoption of electronic health records. Integrating electronic health records and diagnostic tests such as MRIS, genomic sequencing and other technologies provided great opportunities for disease prevention and treatment.[12] Accordingly, guidelines and regulation of data use in health care relate to the creation of a unique global patient ID that can integrate data from a variety of healthcare providers.[12]

HL7 Guidance has been used to provide directives in data sharing / data exchange of health information – especially in relation to electronic health records for research and studying oncologic diseases. However, HIPAA regulations may prevent the complete and open data sharing agreement – hampering research due to patient privacy issues.[12] The use of the single patient identifier seems to be essential for patient data protection using generalized regulation. The authors suggest the creation of a unique global patient ID that can integrate with a variety of health providers.[12]

E. Companies such as Roche - Flat Iron Use Predictive Analytic Tools to Support Patient Data

In viewing patient data in the near future, physicians could be faced with large volumes of data, necessitating electronic records beyond simply patient-physician encounters, to include diagnostic aids.[12] Companies such as Roche – Flat iron are moving toward modeling by building predictive and analytical tools into their electronic health records.[12]

Transparency and portability will remain issues with health care data. The Veteran's Administration has recommended its own strategies for incorporating open access and other physician highlights. However, the solution was not retained due to maintenance and billing issues.[18]

F. Patientory Uses Blockchain and Smart Contracts to Support Patient Data

In relation to other novel patient data security and regulation procedures, Patientory, a health care peer-to-peer electronic medical record (EMR) storage network leveraged blockchain and smart contracts to provide HIPAA compliant health information exchange.[1] Patientory proposed a software framework to address authentication, authorization, access control and data encryption in system implementation and interoperability enhancement.[1]

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 3, pp: (58-66), Month: September - December 2023, Available at: www.noveltyjournals.com

V. CONCLUSION

Jin et al., 2019 rightly presented the challenges related to medical data sharing into the massive amount of data with existing information technology.[1] The integration of data security also has to be combined with issues of confidentiality and integrity. A wide range of governmental regulations including HIPAA, HITECH, The American Recovery and Reinvestment Act of 2009, regulations of the US FDA, and regulations of the Department of Health and Human Services have enacted regulations and protections to secure patient data. Some agencies and acts have also imposed penalties for non-adherence to patient data security and exchange guidelines.

Accordingly, to implement regulations to secure patient data, many organizations have to join forces. Literary reviews have also shown that regulations related to patient data security is an international phenomenon – with overviews of countries and continents such as Sweden, China, the United Kingdom, Europe and Australia.

Likewise organizational strategies and regulations to secure patient data have included administrative, physical and technical safeguards. Specific initiatives for patient data security were included - such as access control, audit trails, backing up data, vetting personnel, security risk analysis, passwords, data encryption, anti-viral software, firewalls and various other forms of authentication.

In addition to organizational strategies and regulations, educators, professional organizations and corporations suggested and implemented regulations in patient data security including publishing documents (Radiology Professional Societies[9]), using single-sign-ons (HL7),[5] incorporating machine learning with electronic medical records (Big Data),[12] building predictive analytic tools into electronic health records (Roche – Flatiron)[12] and providing peer to peer electronic storage network leveraging blockchain and smart contracts (Patientory).[1]

Many strides have been made in regulations related to securing patient data. However, gaps and unknown frontiers remain in relation to health data security of Health 4.0 cloud computing, fog computing, Internet of things (IoT) and telehealth care technologies to share data between various stakeholders.[6]

Future research and strategies will be needed for defining the Internet in terms of cloud computing and patient data. Concepts of the public, private and hybrid cloud will need to be explored including related vulnerabilities.[10] Agrawal and Prabakaran, 2020, identified additional issues for future consideration: fragmentation (when EHRs are unable to communicate effectively with each other); data ownership (regulations, incentives and systems to manage ownership of data); designing a new generation of EHRs (to effectively manage terabytes of data based on years of continuous monitoring); predicative oncologic, and global patient IDs – especially to address proteomics, genomics and metabolomics.[12] Jin et.al 2019 also presented Blockchain based approaches as a means to secure and preserve the privacy of patient data in the age of medical data sharing.[1] As these futuristic initiatives become more active, data security will need to be heightened at an even greater level.

Accordingly, as health data continues to grow and evolve, regulations will be needed to address controversies related to who has the right to access patient data – including third party vendors like insurance companies and employers. Also, united efforts from national and international governmental entities, health care organizations, corporations, educational institutions and more will be needed to assure that patient data is both secure, yet accessible for its intended purpose – which often includes data exchanges, international collaboration and advanced research.

REFERENCES

[1] Jin H., Luo Y, Peilong L., Mathew J. (May 2019). A review of secure and privacy-preserving medical data sharing, IEEE, 7: 61656 – 61669.

[2] Thapa C. and Camtepe S. (February 2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy, Computers in Biology and Medicine, 129:104130.

[3] Liberty University. Health informatics. BUSI/INFO 505. McGraw-Hill Education, 2021.

[4] Duggineni, S. (2023). Information of controls on data integrity and information systems, Science and Technology, 13:2, 29 – 35.

[5] Cucoranu I., Parwani A., West A., Romero-Lauro G., Nauman K., Carter A., Balis U., Tuthill M., and Puntanowitz, L. (January – December 2013). Privacy and security of patient data in the pathology laboratory, Journal of Pathology Informatics, 4:1, https://doi.org/10.4103/2153-3539.108542.

[6] Hathaliya. J. and Tanwar S. (March 2020) An exhaustive survey on security and privacy issues in Healthcare 4.0", Computer Communications, 153:311 – 335.

[7] Rao S., Suma N. and Sunitha M., (2015) "Security solutions for big data analytics in Healthcare", 2015 Second International Conference on Advances in Computing and Communication Engineering. *IEEE*, https://doi.10.1109/ ICA_CCE.2015.83.

[8] Flaumenhaft Y. and Ben-assuli O. (August 2018). Personal health records, global policy and regulation, Health Policy, 122:8, 815 – 826.

[9] Andriole K., (2014). Security of electronic medical information and patient privacy. What you need to know, Journal of the American College of Radiology, 11:12, Part B, 1212 – 1216.

[10] Swede M, Scovetta V. and Eugene-Colin M. (Summer 2019), Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. Journal of Allied Health, 48:2, 148-155.

[11] Sayeed R., Jones J., Gottlieb D., Mandel J., and Mandl K., (2021), A proposal for shoring up Federal Trade Commission protections for electronic health record – connected consumer apps under 21st century cures, Journal of the American Medical Informatics Association, 28:3, 640-645,https://doi.org/10.1093/jamia/ocaa227, 2021.

[12] Agrawal R. and Prabukaran S., (March 2020) Big data in digital healthcare: Lessons learnt and recommendations for general practice, Heredity,124, 525-534.

[13] Zhang L., Wang H., Li Q., Zhao M-H and Zhan Q-M, (2018) Big data and medical research in China, British Medical Journal, 360, 5910.

[14] Honeyman M., Dunn P. and McKenna H., (2016), A digital NHS. An introduction to the digital agenda and plan for implementation". Retrieved from https://www.kingsfund.org.uk/sites/default/files/field/field_publication_file/A_ digital_NHS_Kings_Fund_Sep_2016.pdf.

[15] Snell E., (2017), Healthcare data breach costs highest for 7th straight year.

[16] Rizvi S., Pipetti R., McIntyre N., Todd J., and Williams I. (September 2020). Threat model for securing internet of things (IoT) network at device-level", Internet of Things, 11:10020.

[17] Kruse C. S., Smith B., Vanderlinden H., Nealand A. (2017), Security techniques for the electronic health record, Journal of Medical Systems, 41:127, Retrieved from https://doi.org/10.1007/s10916-017-0778-4.

[18] Garber S., Gates S. M., Keeler E. B., Vaiana M.E., Mulcahy A. W., Lau C., et al., (2014). Redirecting innovation in the U.S. health care: options to decrease spending and increase value, Case Studies, 133.