SecHealth: enhancing EHR security in digital health transformation.

YENG, P., FAUZI, M.A., YANG, B., DIEKUU, J.-B., NIMBE, P., HOLIK, F., KHATIWADA, P., FAHMI, A. and SUN, L.

2023

SecHealth: Enhancing EHR Security in digital health transformation

Prosper K. Yeng
prosper.yeng@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Innlandet, Norway

M Ali Fauzi
moch.ali.fauzi@ub.ac.id
muhammad.a.fauzi@ntnu.no
Brawijaya University
Malang, Jawa Timur, Indonesia
Norwegian University of Science and Technology
Gjøvik, Innlandet, Norway

Bian Yang
bian.yang@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Innlandet, Norway

John-Bosco Diekuu
j.diekuu@rgu.ac.uk
Robert Gordon University
Aberdeen, United Kingdom

Peter Nimbe
peter.nimbe@uenr.edu.gh
University of Energy and Natural Resources
Sunyani, Ghana

Filip Holik
filip.holik@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Innlandet, Norway

Pankaj Khatiwada
pankaj.khatiwada@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Innlandet, Norway

Akbar Fahmi
akbar@dokterpost.com
Nahdlatul Ulama General Hospital
Babat, Jawa Timur, Indonesia

Luyi Sun
luyi.sun@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Innlandet, Norway

ABSTRACT

In the contemporary wave of digital transformation, the implementation of electronic health records (EHRs) has become a pivotal undertaking for numerous nations. However, amidst this technological advancement, a critical facet deserving heightened attention is the security and privacy of these electronic health systems. Regrettably, this crucial concern often finds itself eclipsed by other aspects of digitalization. Consequently, these oversight lapses create vulnerabilities within the EHR framework, leaving them open and exposed to an array of malicious cyber intrusions.

In response to this pressing issue, our study delves into a comprehensive evaluation of security measures within the ambit of African digital health strategies. Remarkably, among the number of approximately 42 nations that have embarked on digital health strategy formulation, a mere 2 countries have taken cognizance of the imperative to integrate robust security and privacy policies into their healthcare-oriented digital transformation initiatives.

In light of this disconcerting revelation, we present an actionable roadmap that endeavours to fortify EHR security, aligning with the progressive "shift-left" paradigm. By advocating for the proactive integration of security measures from the inception of EHR development, we strive to curtail vulnerabilities and enhance the overall resilience of these systems. Our proposed roadmap stands as a clarion call for governments, healthcare authorities, and technology stakeholders to collectively prioritize security in tandem with digital health advancement, thereby fostering a safeguarded and privacy-respecting electronic healthcare landscape.

CCS CONCEPTS

• **Security and privacy** → **Domain-specific security and privacy architectures**; *Vulnerability management*.

KEYWORDS

Healthcare, Cybersecurity, Threat modeling, Threat identification

ACM Reference Format:
Prosper K. Yeng, M Ali Fauzi, Bian Yang, John-Bosco Diekuu, Peter Nimbe, Filip Holik, Pankaj Khatiwada, Akbar Fahmi, and Luyi Sun. 2023. SecHealth: Enhancing EHR Security in digital health transformation. In *International Conference on Sustainable Information Engineering and Technology (SIET 2023), October 24–25, 2023, Badung, Bali, Indonesia.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3626641.3627214

1 INTRODUCTION

The field of digital health has witnessed remarkable growth and development in recent years, transforming the way healthcare services are delivered and accessed globally. The adoption of Electronic Health Records (EHR) stands as a pivotal milestone in this digital revolution, promising improved patient outcomes, streamlined workflows, and enhanced overall efficiency in the healthcare sector. The International Organization for Standardization (ISO) defines an EHR as a catalogue of patient information, in computer-processable form, stored and transmitted securely such that it is accessible by

SIET 2023, October 24–25, 2023, Badung, Bali, Indonesia

ACM ISBN 979-8-4007-0850-3/23/10.
https://doi.org/10.1145/3626641.3627214

multiple authorized users [8]. As countries worldwide embrace this transformative trend, it becomes evident that digital health is not just a modern convenience but a necessity for modernizing healthcare systems.

The significance of digital health transformation is evident from the global momentum it has garnered. Numerous countries have recognized the potential benefits of digital health and have taken proactive steps to prioritize its implementation. One of the most notable examples is the initiative launched by former U.S. President Obama, which allocated a staggering $18 billion to incentivize physicians to adopt the EHR system [9]. This landmark decision marked a turning point in the history of healthcare, emphasizing the critical role of digital health in improving healthcare services and outcomes.

In Asia, countries like Indonesia have made significant strides by mandating the adoption of EHR in all healthcare facilities by the end of December 2023 [13]. This forward-thinking approach aims to enhance health governance, streamline healthcare services, and improve patient outcomes through better access to data and data integration. Meanwhile, the impact of digital health transformation is also evident in Africa, where the DHIS2 electronic health record system, pioneered by the University of Oslo, has gained widespread adoption across the continent. Countries like Ghana, Tanzania, and Liberia have embraced DHIS2, paving the way for improved healthcare delivery and management in the region [7]. The move towards digital health solutions in Africa is driven by the recognition of the benefits they offer, including improved service quality, streamlined workflows, cost and time savings, and enhanced overall efficiency in the healthcare sector. Digital transformation as shown in Figure 5 encompasses "three Ds" thus digitization, digitalization and digital transformation stages. Digitization involves the conversion of analogue or physical data into digital form while digitalization involves automation by employing digital technologies such as artificial intelligence tools. Automation by using digital tools for instance requires digital records, hence the need for digitization in the digital transformation process.

Despite all these benefits offered by EHR, security and privacy have become a significant concern; from patient privacy invasion to hacking and ransomware attack. In Indonesia, the COVID-19 database and the health insurance system were recently hacked, breaching the confidentiality integrity and availability of these systems [6]. In Finland, the patient information system was hacked and the adversaries demanded payments from each of the patients otherwise their patient information was to be published on social media [10]. In Norway, a healthcare professional was recently dismissed for snooping into her lover's ex-wife's medical records [14]. Aside from that, about 3 million medical records were breached in Norway and the citizens were perturbed about the incident.

While digital transformation is essential for accelerated efficiency in the healthcare sector, the security and privacy assurance of the systems need to be deeply considered. Security assurance is the confidence that the security requirements are met by a system based on specified evidence provided by the assurance system [12]. The security requirements of most systems are not comprehensively considered, as some aspects of security requirements, vulnerability or threats are considered instead. The incomprehensiveness of incorporating security requirements can open up an EHR system to various kinds of privacy and security invasions. There are general security evaluation methods and standards including OpenSAMM, BSSIM, common criteria (CC), and standard vulnerability scoring scheme (CVSS) [12]. However, these methods provide the foundation for assessing security requirements in a system without considering the domain or context [1, 26]. Prioritizing security requirements based on the context such as healthcare has been considered to be very essential in the system development life cycle. Also, these methods focused more on the processes than the technical implementation assessment.

This paper assessed the concept of digital health transformation in Africa, focusing on digital health strategies and their security measures. Having been encouraged by the World Health Organization, there have been recent vigorus digitalization initiatives in Africa [19]. This study provided answers to the following research questions: 1) What is the extent of incorporating security and privacy in EHR of digital health transformation in Africa? 2) How can EHR security be efficiently enhanced in countries adopting these systems?

Therefore, we propose a road map for effectively enhancing security measures in EHR, delving into the various aspects of digital transformation in healthcare, initiatives undertaken in Africa, and the existing challenges and gaps.

Section 2 of the paper provides the approach that was used to provide the road map. Section 3 focuses on findings such as the specific DT initiatives that have been undertaken in Africa, with a particular emphasis on the adoption and impact of EHR systems. The challenges and gaps faced by African nations in their digital health transformation journey were also critically analysed in this section.

Finally, Section 4 will propose a comprehensive way forward, outlining a framework for effectively incorporating security requirements for EHR systems. This framework will consider international best practices while accounting for the specific needs and challenges of various continents.

2 METHODS

To contribute towards enhancing the security of EHR, we assessed the digital health strategies in Africa. Fifty-four African countries' digital strategies were assessed for strategies developed, digital transformational areas, and security strategies adopted for healthcare in their respective digital health strategies. Additionally, reviewed related work in Google Scholar, IEEE Explore, Scopus and PUBMED.

3 RELATED WORK

EHR systems are increasingly becoming attractive solutions to most countries' healthcare systems. However, this comes with eminent security implications such as an increase in attack surface, leading to data breaches, medical record snooping and ransomware attacks if the security requirements are not sufficiently considered. The security requirement of an EHR system may include the security of the hosting network infrastructure, the hosting computing server security, physical security, human factors and software security, but, this paper focused on the software security aspect of the EHR system.

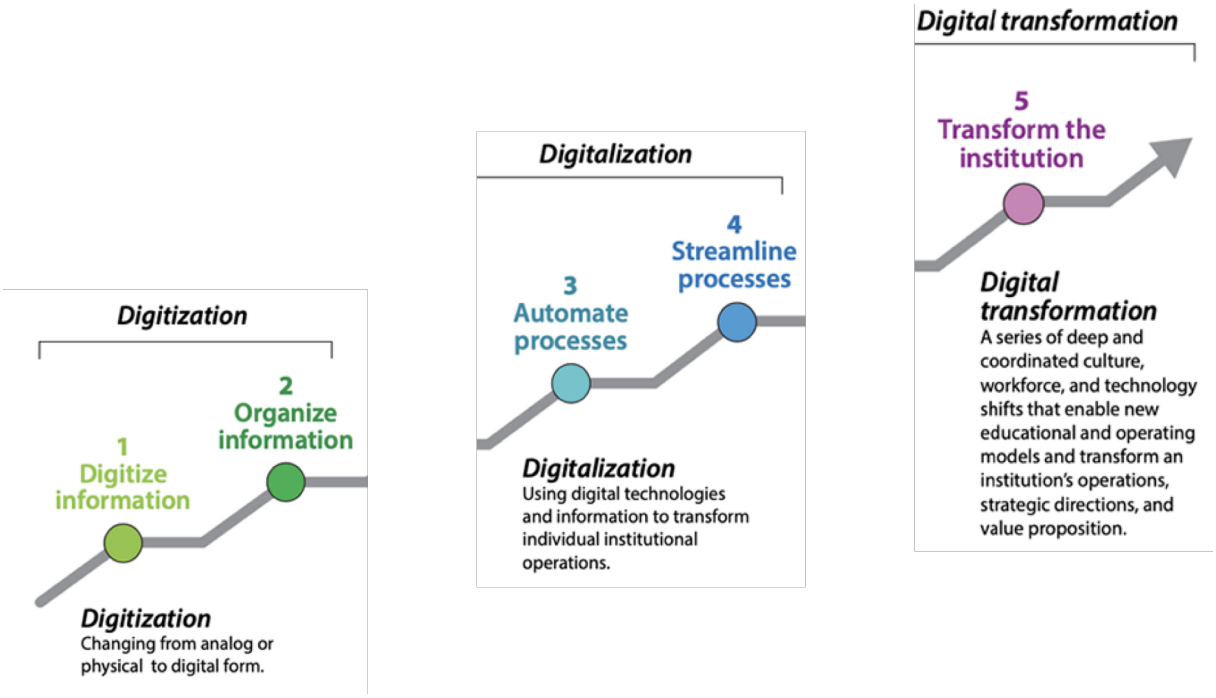

Figure 1: Digital transformation [11]

In a study conducted by Austin et al. [5], certification standards from accredited bodies like the Certification Commission for Health Information Technology in the USA were examined. The study revealed that while security criteria largely focused on design flaws, issues related to implementation bugs were disregarded. This was highlighted by evaluating an open-source electronic health record system (OpenEMR) certified by an authorized body. The outcomes revealed a significant number of true positive implementation flaws within the application, encompassing issues such as cross-site scripting and insecure cryptographic algorithms. Similarly, the mode of evaluating security assurance was highlighted by Katt and Prasher [12]. They intimated that the current use of qualitative means in measuring the confidence of a system is costly and time-consuming, which can not be used by small-medium enterprises (SMEs). Hence, a quantification method was proposed to test the confidence level of systems. Two case studies were applied to their method using REST APIs developed by Statistics Norway, and the outcomes showed that the API with the most security mechanisms implemented got a slightly higher security assurance score. Almulhem [4] proposed a threat modelling methodology called attack tree to analyze attacks affecting EHR systems. The analysis was based on a generic client-server model of EHR systems. The model proved positive in performing quantitative and qualitative analysis in identifying countermeasures such as user authentication, timeout policy, access revoke policy, user authorization, encryption, and security awareness. Likewise, Abomhara et al. [2] performed threat modelling to identify possible threats to telehealth systems to help enhance system security. They used the Microsoft threat modelling tool 2014 to model the telehealth systems. Based on the outcome, various countermeasures were identified relating to authentication, authorization, access, and privacy, as well as auditing and logging threats for implementation.

These studies [2, 4, 5, 12] provided in-depth evaluation for security assurance however, these methods did not cover all aspects of EHR development processes to identify, design, implement and test or evaluate for security incorporation. Again, state-of-the-art software development has a backend server hosted with application development interfaces (APIs) where the front-end server such as React.js tend to interact with the backend for CRUD operations. Aside from [12] who assessed the security of the APIs, non of the above studies considered the security in this separation of the back-end from the front-end.

Puppala et al. [18] proposed a security and privacy model that examined how large biomedical databases could allow queries for aggregate patient cohort numbers without exposing patient identities. The authors used Methodist Environment for Translational and Outcomes Research (METEOR) tool, which is made up of enterprise data warehouse (EDW) and a software intelligence and analytics (SIA) layer to test various eHealth apps, including mPOD (Query Tool), READMIT (Readmission Risk Tool), MOCHA (Methodist Hospital Cancer Health App), and MINIMA (Weight management app). While privacy in relation to data retrieval was considered, the security, of EHR was not comprehensively delt with.

4 SECURITY REQUIREMENT GAPS IN DIGITAL HEALTH STRATEGIES IN AFRICA

Following these shortcomings, we assessed the digital health strategies of Africa to determine the security strategies enshrined. As shown in Figure 2,

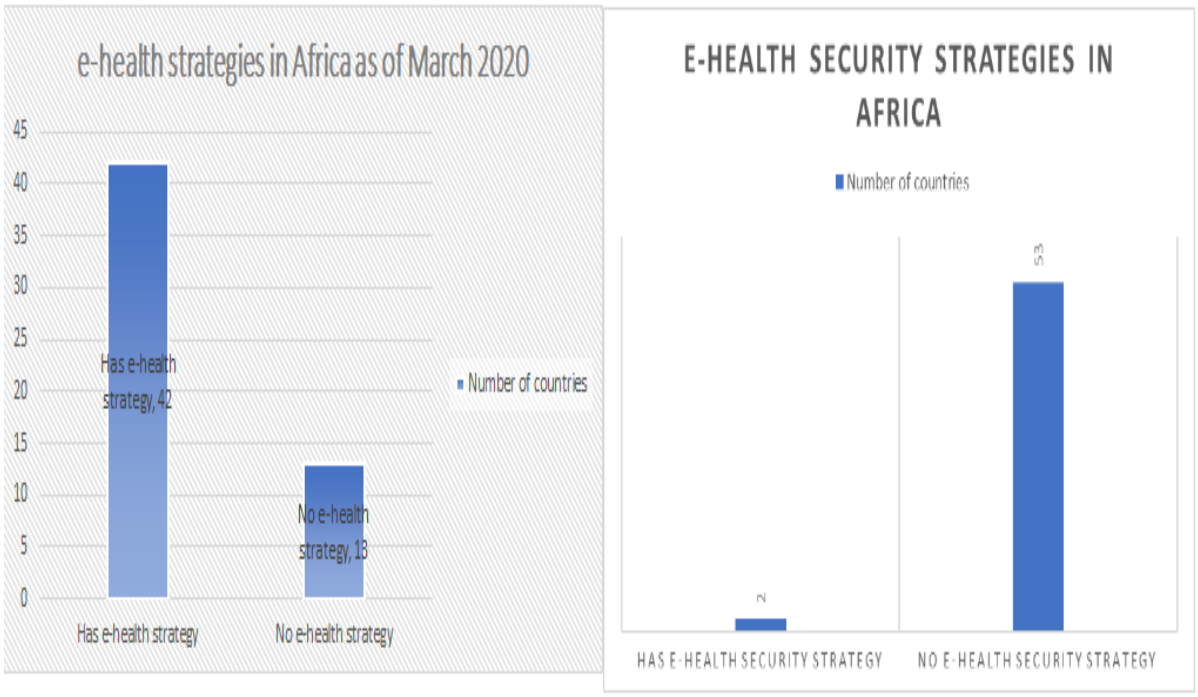

Figure 2: e-Health strategies and security considerations

out of 54 African countries, about 42 (78%) developed digital health strategies. Meanwhile, among the 42 countries that developed digital health strategies, only 2 of them further developed healthcare-specific security strategies or policies.

According to WHO, about 12 countries implemented their strategies but relied on at least some generic security regulations such as their national cyber security regulations. A grain of evidence of the level of security incorporation can be traced in Figures 3 and Figure 4. Figure 3 depicted five implementation stages of a particular country's digital health implementation stages starting from experimentation, early adoption, development and building up, scale-up and mainstreaming.4

Out of these stages, the implementation of the eHealth system is in the 3rd stage corresponding to development and building up. Meanwhile, security development has not been considered simultaneously as shown in Figure 4.

5 WAY FORWARD TOWARDS ENHANCING SECURITY IN EHR

Following the security gaps that were identified in the digital transformational efforts in Africa, we propose a comprehensive approach towards enhancing secure EHR development. This includes a threat-driven approach [15], incorporating shift-left in cyber security by considering the people, technology and processes in the development phases of any typical software development methodology. The security considerations in this approach include Security requirement gathering and analysis, identification of assets, threat modelling, risk management, security orientation, managing secure coding, security testing, security maintenance and operation, and security disposition [20]. These are infused in the software development life-cycle as depicted in Figure 5.

Human factors including intentional and unintentional action can increase attack surface. Especially, in recent EHR systems where patients tend to have access to the system. So cybersecurity training and awareness are essential for all those who are involved in the development and use of the system. Project team members including project managers, system analysts, developers and testers need to be trained to understand the potential risks, their roles and responsibilities, and how their actions can impact the overall security of the EHR product. Furthermore, usability problems can tend to undermine security controls where for instance the healthcare staff can tend to skew to sharing passwords [23].

The process aspect of the 3 pillars in security measures deals with procedures, legal and regulatory requirements, security standards, business needs and policies in developing security and privacy requirements in EHR [21, 25]. These can range from basic consent management policies to complex disaster recovery and business continuity plans. The technology aspects include API security, access control, and cryptographic technologies for hashing and encryption. [24].

In the realm of software development methodologies, the conventional process involves sequential steps such as requirement gathering, design, implementation, testing, acceptance, production, and maintenance [16]. To address the imperative need for

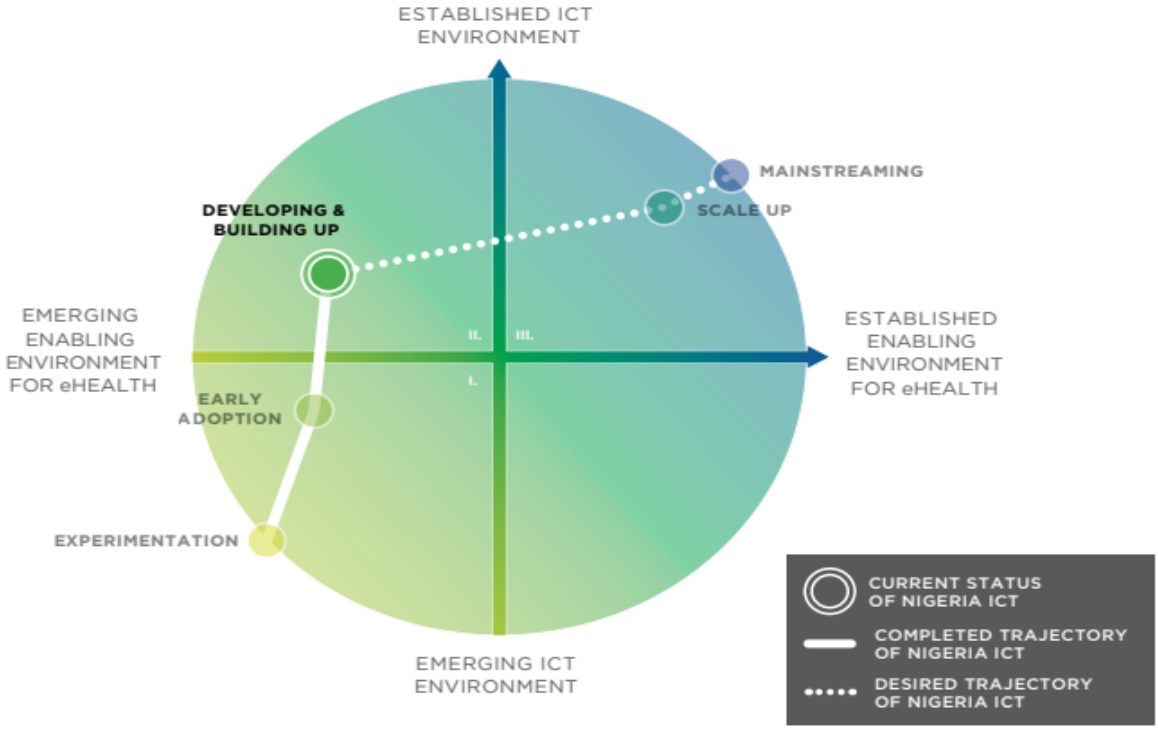

Figure 3: emplementation-stage of a particular country

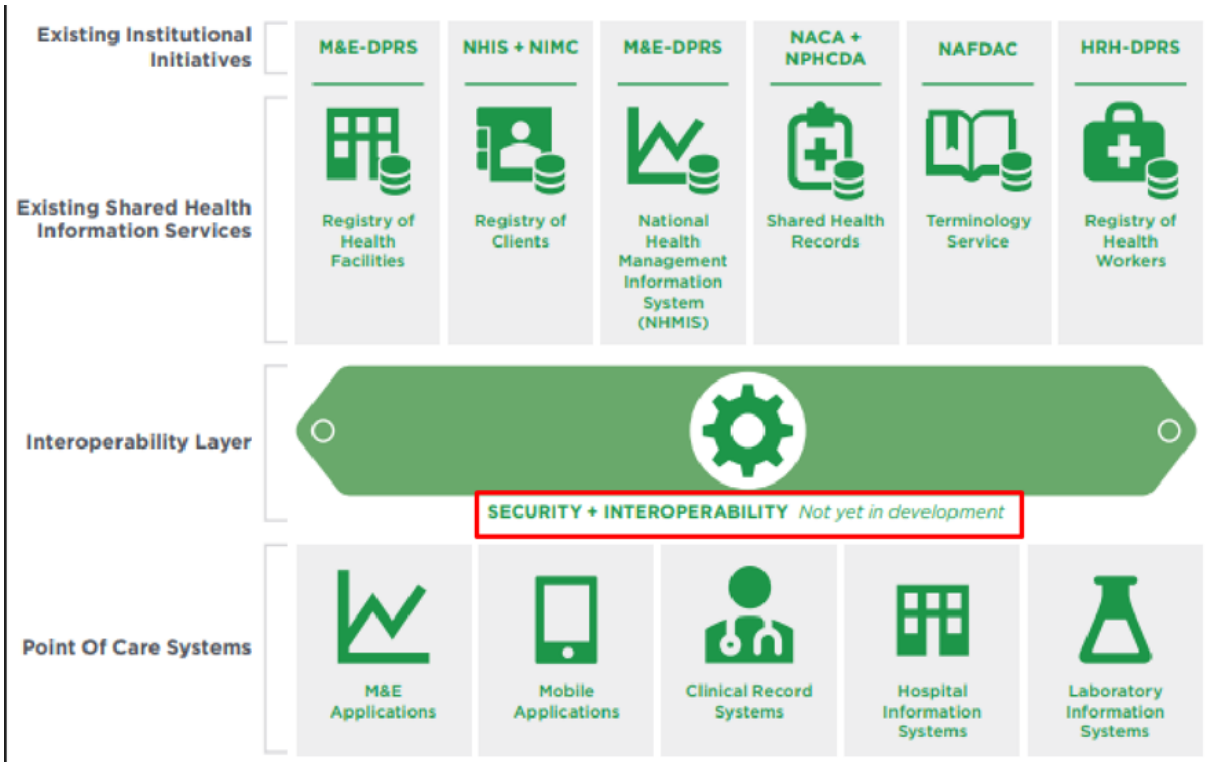

Figure 4: Security implementation stage

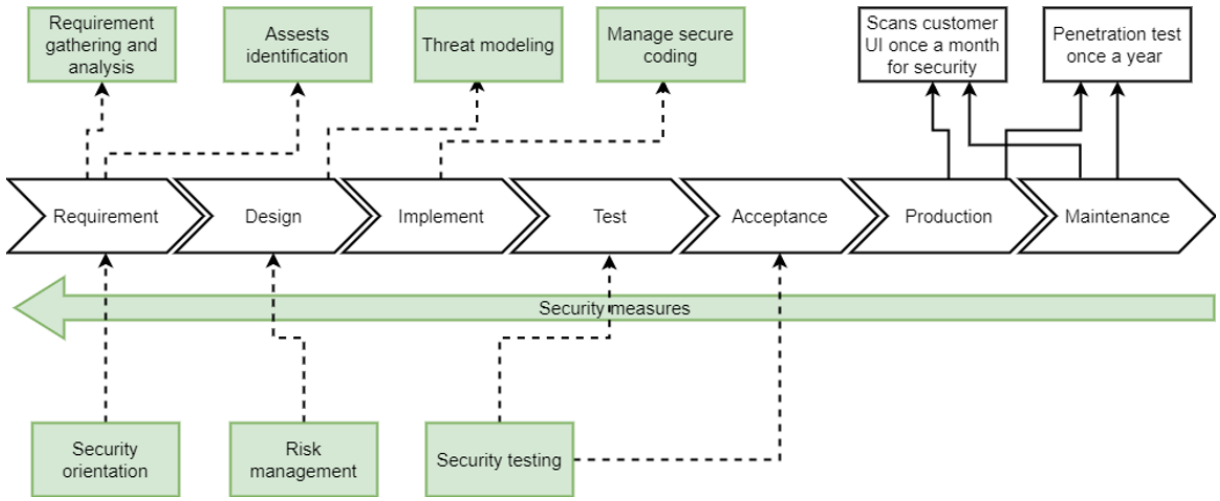

Figure 5: Shift-Left frame work

robust security measures, a paradigm shift towards a proactive and holistic approach is essential. We propose an innovative security-centric framework that seamlessly integrates security practices into the software development life cycle, amplifying the software's resilience against potential threats and vulnerabilities. At the same time, our framework follows the service design principle which is holistic and human-centered [27]. It ensures the usability of the system.

Our proposed framework, referred to as the "Holistic Enhanced Security Development Framework in Healthcare," goes beyond conventional security integration by embracing a "shift-left" strategy [17]. Unlike traditional approaches, our methodology emphasizes the early infusion of security considerations throughout the software development life cycle, creating a proactive defense mechanism against security breaches and exploits. This approach is distinct from other systems due to its strategic emphasis on:

Security Orientation and Early Training: At the outset of the requirement-gathering phase, our framework emphasizes security orientation sessions to ensure that all project team members understand their responsibilities in upholding security measures. This early training not only enhances awareness but also fosters a security-conscious mindset from the project's inception.

Comprehensive Asset Identification: Identifying software assets is fundamental to comprehending the scope of potential threats and vulnerabilities. In contrast to conventional practices, our framework goes beyond mere identification to assess the inherent threats and vulnerabilities associated with each asset. This proactive approach enables tailored security measures for different assets.

Threat Modeling and Vulnerability Identification: Leveraging various sources such as legal regulations, business objectives, maturity models, and security standards, our framework incorporates an elaborate threat modelling process. In addition to conventional techniques, our approach integrates established resources like OWASP's top ten vulnerabilities list, facilitating a more exhaustive vulnerability identification process [22].

Rigorous Risk Management and Mitigation: Our framework introduces an enhanced risk assessment process, wherein identified risks serve as the foundation for making informed mitigation decisions. Unlike conventional approaches that often focus on risk transfer or avoidance, our methodology encompasses an array of choices including control implementation and acceptance, thus ensuring a comprehensive risk management strategy.

Integrated Socio-Technical Measures: Recognizing that software security extends beyond just technological aspects, our framework encompasses socio-technical measures to address the human and social dimensions of security. This integration ensures a holistic approach that considers not only technological vulnerabilities but also behavioural and organizational aspects.

Multi-dimensional Security Testing [5]: In the testing and acceptance phases, our framework endorses a multi-pronged security testing strategy. This includes a combination of black box, white box, static, and dynamic testing, conducted through both manual and automated means. This exhaustive testing approach significantly enhances the likelihood of identifying potential gaps and vulnerabilities.

Continual Security Maintenance: Post-production and during maintenance phases, our framework mandates regular security maintenance activities. These activities involve vulnerability scanning and penetration testing, ensuring that the software remains fortified against evolving threats throughout its lifecycle.

Comprehensive Component Considerations: Acknowledging the complexity of modern software systems, our framework underscores the importance of encompassing various components—ranging from in-house APIs and front-end UI components to external APIs, plugins, and databases—within the security management process. This comprehensive approach reduces blind spots and potential entry points for attackers.

To ensure the robust security of Electronic Health Records (EHRs), it is imperative to establish an effective security certification process. This involves a thorough evaluation that encompasses misuse cases, static analysis, and dynamic analysis.

Misuse cases are like scenarios where potential attackers exploit vulnerabilities. By comprehensively assessing EHRs through misuse cases, we proactively identify weak points that could be targeted. This approach enables us to anticipate potential threats and address vulnerabilities before they can be exploited. It's like strengthening a fortress by finding weak spots before the enemy does.

Static analysis is like examining the blueprints of a building. We analyze the EHR's source code and design without actually running it. This process helps us uncover hidden flaws and security gaps that might not be obvious when the system is running. It's akin to finding hidden traps in a maze before anyone steps in [5].

Dynamic analysis is like testing a car's safety features by driving it. We observe how the EHR behaves when used actively [3, 5]. This helps us identify real-time vulnerabilities and threats that might only surface during actual usage. It's similar to discovering how a ship handles rough waters by actually sailing it.

6 CONCLUSION AND LIMITATIONS

EHR aspect of digital transformation could be one of the most vital aspects of digital transformation. Therefore, the Holistic Enhanced Security Development Framework in Healthcare is a revolutionary approach that diverges from conventional software security methodologies. By infusing security practices early in the development life cycle and considering a multi-dimensional spectrum of security aspects, our framework exemplifies a proactive stance against the ever-evolving landscape of cyber threats.

REFERENCES

[1] Ala A Abdulrazeg, Norita Md Norwawi, and Nurlida Basir. 2017. RiskSRP: Prioritizing Security Requirements Based on Total Risk Avoidance. *Advanced Science Letters* 23, 5 (2017), 4596–4600.

[2] Mohamed Abomhara, Martin Gerdes, and Geir M Køien. 2015. A stride-based threat model for telehealth systems. *Norsk informasjonssikkerhetskonferanse (NISK)* 8, 1 (2015), 82–96.

[3] Ahmad Almulhem. 2011. Threat Modeling for Electronic Health Record Systems. *Journal of medical systems* 36 (08 2011), 2921–6. https://doi.org/10.1007/s10916-011-9770-6

[4] Ahmad Almulhem. 2012. Threat modeling for electronic health record systems. *Journal of medical systems* 36 (2012), 2921–2926.

[5] Andrew Austin, Ben Smith, and Laurie Williams. 2010. Towards improved security criteria for certification of electronic health record systems. In *Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care*. 68–73.

[6] bizbridge. 2023. Hacker Bjorka Claimed to Breach Indonesia's Data. https://bizbridge.id/news/read/hacker-bjorka-claimed-to-breach-indonesia-s-data

[7] DHIS2. 2023. *Monitoring regional health data in West Africa.* Retrieved August 3 2023 from https://dhis2.org/waho-uses-dhis2/#

[8] International Organization for Standardization. 2005. *Health informatics-Electronic health record-Definition, scope and context.* na.

[9] Ralph Grams. 2012. The Obama EHR experiment. , 951–956 pages.

[10] The Guardian. 2020. Shocking hack of psychotherapy records in Finland affects thousands. https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland

[11] JISC. 2023. Digital at the core: a 2030 strategy framework for university leaders. https://www.jisc.ac.uk/guides/digital-strategy-framework-for-university-leaders/what-is-digital-transformation

[12] Basel Katt and Nishu Prasher. 2018. Quantitative security assurance metrics: REST API case studies. In *Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings*. 1–7.

[13] Healthcare Asia Magazine. 2023. Indonesia Mandates Its Healthcare Facilities To Use EMRs. Retrieved August 03 2023 from https://healthcareasiamagazine.com/exclusive/indonesias-journey-towards-electronic-medical-records

[14] Mondag. 2022. Norway: Medical Record Snooping Was Reason For Termination. https://www.mondaq.com/health--safety/1148214/medical-record-snooping-was-reason-for-termination

[15] Michael Muckin and Scott C Fitch. 2014. A threat-driven approach to cyber security. *Lockheed Martin Corporation* (2014).

[16] OWASP. 2023. *SAMM model overview.* Retrieved April 6 2023 from https://owaspsamm.org/model/

[17] Mark Pitchford. 2021. The 'Shift Left'Principle.

[18] Mamta Puppala, Tiancheng He, Xiaohui Yu, Shenyi Chen, Richard Ogunti, and Stephen TC Wong. 2016. Data security and privacy management in healthcare applications and clinical data warehouse environment. In *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*. IEEE, 5–8.

[19] WHO. 2021. Framework for implementing the global strategy on digital health in the WHO African Region: report of the Secretariat. hhttps://apps.who.int/iris/handle/10665/345393

[20] Prosper Yeng, Stephen D Wolthusen, and Bian Yang. 2020. Comparative analysis of threat modeling methods for cloud computing towards healthcare security practice. (2020).

[21] Prosper Yeng, Bian Yang, and Einar Snekkenes. 2019. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2. IEEE, 397–404.

[22] Prosper Yeng, Bian Yang, Terje Solvoll, Peter Nimbe, and Benjamin Asubam Weyori. 2019. Web Vulnerability Measures for SMEs. (2019).

[23] Prosper Kandabongee Yeng, Muhammad Ali Fauzi, Luyi Sun, and Bian Yang. 2022. Assessing the legal aspects of information security requirements for health care in 3 countries: Scoping review and framework development. *JMIR Human Factors* 9, 2 (2022), e30050.

[24] Prosper Kandabongee Yeng, JK Panford, James Ben Hayfron-Acquah, and Frimpong Twum. 2016. An efficient symmetric cipher algorithm for data encryption. *Int Res J Eng Technol* 3, 05 (2016), 8–9.

[25] Prosper Kandabongee Yeng, Bian Yang, and Monica Stolt Pedersen. 2022. Assessing cyber-security compliance level in paperless hospitals: An ethnographic approach. In *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE, 1–8.

[26] Sang Guun Yoo, Hugo Pérez Vaca, and Juho Kim. 2017. Enhanced misuse cases for prioritization of security requirements. In *Proceedings of the 9th International Conference on Information Management and Engineering*. 1–10.

[27] Eun Yu and Daniela Sangiorgi. 2014. Service Design as an approach to New Service Development: reflections and future studies.