Proc. of the International Conference on Electrical, Computer and Energy Technologies (ICECET)
9-10 December 2021, Cape Town-South Africa

Integrating Privacy-By-Design in e-Health

Vincent Amankona
Department of Computing and Information Sciences
Catholic University College of Ghana
Sunyani, Ghana
vincent.amankona@cug.edu.gh

Audrey Asante
Department of Computing and Information Sciences
Catholic University College of Ghana
Sunyani, Ghana
audrey.asante@cug.edu.gh

Michael Opoku
Department of Computing and Information Sciences
Catholic University College of Ghana
Sunyani, Ghana
michael.opoku@cug.edu.gh

Patrick Ohemeng-Gyaase
Department of Computing and Information Sciences
Catholic University College of Ghana
Sunyani, Ghana
pkog@cug.edu.gh

Clement Srekumah
Department of Decision Science and Applied Mathematics
Catholic University College of Ghana
Sunyani, Ghana
clement.srekumah@cug.edu.gh

Alex K. Peprah
Department of Decision Science and Applied Mathematics
Catholic University College of Ghana
Sunyani, Ghana
alex.peprah@cug.edu.gh

Philip Amankwa-Danquah
Department of Computing and Information Sciences
Catholic University College of Ghana
Sunyani, Ghana
amankwah.danquah@cug.edu.gh

2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) | 978-1-6654-4231-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICECET52533.2021.9698489

***Abstract*— Technology has changed how services are provided and activities are performed in today's world. The increased usage of technology has resulted in the development of hardware and software-based solutions. The healthcare industry, which cannot be left out, also uses these hardware and software-based solutions to perform activities and provide services. Some African countries have also adopted these solutions to provide healthcare to their citizens. The reliance on technology requires the tackling of security and privacy issues. As a developing continent with fragile health systems, adopting e-health presents numerous security and privacy concerns that must be addressed. Privacy by Design, which is regarded as a privacy protection paradigm, is critical for African countries that want to or have already adopted e-health. Therefore, the adoption of e-health necessitates the implementation of Privacy by Design to mitigate security and privacy incidents. In this study, we propose a Privacy by Design framework for e-health. The framework consists of the following components: management, people, technology, and users. The proposed framework is intended to improve privacy by design procedures when implementing e-health. This framework would ensure to improve privacy protection as well as information security. Integrating privacy by design into e-health will improve the handling of security and privacy incidents while also protecting personal data and privacy.**

Keywords*— *Privacy by design, e-health, security

I. INTRODUCTION

The healthcare delivery system is critical to the survival of the human race, and its effectiveness is determined by the reliability of health information. Over the years, the healthcare system has evolved from traditional service delivery to more effective services in which reliable decisions are made using electronic support health systems. According to [1], all healthcare services necessitate the use of information and communication technology (ICT) to ensure effective service delivery. e-Health as defined by [2] is the implementation of ICT into healthcare delivery to collect, process, store, retrieve, and communicate a large volume of health information to various health domains. e-Health was introduced to improve the quality of healthcare service delivery and to help overcome the limitations of the traditional book record-keeping system [3]. The introduction of e-health has strengthened the health system by providing e-health records and diagnosis applications to aid in the day-to-day operations of the healthcare system [4], [5]. It has also made it possible to implement strategic health policies and effective health intervention planning systems to improve a country's overall health conditions and support its people's growth and standard of living. In their studies, [6] and [7] concluded that findings from developing countries indicated that e-health systems enabled easy access to healthcare facilities and effective healthcare delivery by healthcare practitioners. Imagine how much easier life would be for health practitioners and the emergency unit if complete patients' medical data, including their conditions, required treatments, and procedures could be easily made available to them upon request.

On the contrary, e-health raises concerns about privacy in terms of access, processing, storage, transmission, integrity, and overall security. Some communication channels may be untrustworthy, while others may have unsecured access, allowing unauthorized disclosure of a person's health information. Unsecured e-Health systems can be more dangerous if an adversary has access to them, such as illegally processing patients' health data [8]. Therefore, when implementing e-health, it is critical to use privacy-by-design procedures to address security and privacy concerns. Privacy by design (PbD) refers to the proactive incorporation of good privacy and data protection processes into the design and operation of an IT system. PbD aims to protect users' privacy and data, allowing them to gain trust in the systems.

This paper aims to propose privacy by design framework for e-health. This framework ensures and improves privacy and information security in the health sector. This paper also evaluates issues and challenges that must be addressed when implementing e-health. Addressing these issues and challenges will improve Africans' access to better healthcare.

II. Background

This section reviews related works on privacy by design and e-health.

A. Privacy by Design (PbD)

"Privacy by Design" refers to a set of guidelines that can be used from the beginning of the development of a system to address privacy concerns and ensure data protection compliance. The privacy by design framework was published in 2009 and adopted by the International Assembly of Privacy Commissioners and Data Protection Authorities in 2010 [9]. According to [9], PbD connotes a deliberate fusion of technical privacy principles into a system's design and the acknowledgment of privacy in a company's risk management processes. Privacy by design calls for privacy to be considered throughout the whole engineering process. Therefore, PbD can be defined as "an engineering and strategic management approach that commits to selectively and sustainably minimize information systems' privacy risks through technical and governance controls." [9].

Design of systems for the protection of peoples' data must purposefully be focused on to embrace PbD. Accordingly, privacy must be on systems' requirements radar from the start of a new project. It needs to enter the system development life cycle at such an early point that architectural decisions around data processing, transfer, and storage can still be made. Managers and designers (along with other potential stakeholders) must assess the privacy risks they are willing to accept and agree on technical and governance controls for the risks they are unwilling to bear.

Principles of Privacy by Design

Privacy by Design affirms the international principles of Fair Information Practices (FIPs) but outweighs it to attain the greatest global standard possible. PbD represents a considerable "raising" of the bar in the field of privacy protection. The 7 Foundational Principles of Privacy by Design as advanced in [9] are presented below:

a) Proactive rather than reactive measures; preventative rather than remedial: The PbD approach foresees and prevents invasions of privacy before they occur. PbD does not wait for privacy concerns to arise, nor does it provide remedies for resolving privacy violations after they have occurred; instead, it tries to avoid them. In other words, PbD occurs before, not after, the event.

b) Privacy as the Default Setting: By guaranteeing that personal data is automatically protected in any given IT system or business activity, PbD aims to provide the highest level of privacy. Even if a person does nothing, their privacy is protected. Individuals do not need to take any action to protect their privacy because it is already incorporated into the system.

c) Privacy Embedded into Design: PbD is a concept that is included in the design and architecture of IT systems as well as business processes. It is not considered later as an afterthought. As a result, privacy thus becomes a critical component of the basic functionality provided.

d) Full Functionality – Positive-Sum, not Zero-Sum: PbD aims to accept all legitimate interests and purposes in a positive-sum "win-win" approach, rather than an outmoded, zero-sum approach that involves unnecessary trade-offs. PbD dispels the myth of false dichotomies like privacy vs. security, illustrating that the two may coexist.

e) End-to-End Security – Full Lifecycle: This ensures that all data is safely maintained and then safely erased promptly at the end of the process. As a result, PbD ensures secure information lifecycle management from beginning to end.

f) Visibility and Transparency - Keep it Open: PbD aims to reassure all stakeholders that whatever business practice or technology is in use, it is operating per the stated promises and objectives and that this is subject to independent verification. Users and suppliers alike can see and understand its component pieces and operations. Always remember to trust but double-check.

g) Respect for User Privacy – Keep it User-Centric: Above all, PbD requires architects and operators to prioritize the needs of individuals by including features such as strong privacy defaults, adequate notice, and empowering user-friendly options. Maintain a user-centered approach.

B. e-Health

E-Health refers to health services and information provided or implemented via the internet and similar technologies. A broader interpretation of the term was proposed by [10] as "a state-of-mind, a way of thinking, an attitude, and a commitment to networked, global thinking to improve health care locally, regionally, and globally through the use of information and communication technology."

e-Health is the most reliable means of meeting the fastest-growing health demand in our time [8]. The benefit of e-Health has been significant: lower health-care costs, faster and more direct patient service, and increased transparency at all levels [8]. E-health systems are capable of transmitting personal (patient) data to physicians by indicating the diverse physiognomies of the human body such as blood pressure, temperature, physical fitness, medication, and the location of the person.

Though e-health has many advantages, it also has security and privacy issues that must be addressed.

C. e-Health and Privacy Policies in Africa

Africa, a continent consisting of four sub-regions, is making significant progress in terms of developing and implementing technology-driven health advances. As improvements in e-

Health result in growing levels of data gathering and surveillance, policymakers are increasingly realizing the increasing concerns for online personal privacy and data protection [11]. While e-Health advances are crucial for the provision of healthcare services in African countries, they can also pose substantial hazards to users' online privacy because the information shared in e-Health applications contains some of the most personal and sensitive facts about a person's life. More so, data breaches can cause significant harm, including direct effects on employment, insurance coverage, and physical safety [12].

As a result, several African countries recognize the legal necessity of protecting the privacy of their residents' (health) information. Only a few countries, including Ghana, Mauritius, Morocco, South Africa, and Tunisia, have established comprehensive legislative frameworks with effective enforcement mechanisms [11]. At the same time, little is known about the general public's understanding of privacy policies across the continent. Few studies have looked into the state of privacy and data protection in Africa, particularly e-Health privacy laws [11], [13]–[15]. Reference to these studies, e-Health regulation is either non-existent, difficult to access, or fragmented [15]. Even existing privacy and data protection legislation is sometimes ambiguous, immature, in the process of being prepared, or yet to be passed by legislative bodies [16].

In 2014, the AU set up the Convention on Cybersecurity and Personal Data Protection that prescribed security rules for electronic exchanges, individual information insurance, and cybercrimes, to more readily ensure the protection of residents across the landmass and address the perils and dangers derived from the utilization of electronic information and individual records in their day by day and expert lives (African Union, 2014. Sadly, this document is heavily influenced by the now-outdated European Union data protection directive (directive 95/46/EC) (The European Parliament, 1995).

The ECOWAS sub-region urges each member state to establish a data protection authority to oversee the implementation of the specified data protection regulation(s), protect user privacy, and promote the free flow of information among member states and non-ECOWAS member states with equally adequate privacy protection [11]. Five Southern African Development Community (SADC) member states [Seychelles, Mauritius, Angola, Lesotho, and South Africa] have implemented robust data privacy legislation, as well as a more precise and consistent Data Protection Model-Law 2012, which contains a specific policy on the automatic and non-automatic processing of both private and public data [17]. In contrast to the aforementioned African sub-regions, [18] and [17] asserted that the Economic Community of Central African States (ECCAS) has the least established data privacy policies.

According to [15] impact study on African e-Health Regulation, e-Health has mostly flourished without the benefit of any unique formal law explicitly adapted to its application across the continent. This analysis of e-Health legal frameworks in ten African countries (Ivory Coast, Ghana, Kenya, Malawi, Mozambique, Nigeria, Rwanda, Tanzania, Uganda, and Zambia) found that, while legal frameworks differed between countries and African regions, all of these countries' constitutions recognized the right to health in some way.

In general, most African countries lack concrete data and privacy protection regulations. Only 21 African countries have enacted privacy legislation, which is heavily influenced by out-of-date European standards [18]. As a result, there are no specific provisions in these laws that cover e-Health privacy; instead, protections must be derived from generic privacy and/or healthcare legislation, where applicable. As a result, particular privacy and data protection guidelines and rules for e-Health technologies are required. African countries should examine their legal systems for flaws and take appropriate steps to rectify them. Standardization and harmonization of definitions for various data types or concepts, such as "sensitive data," "health or personal data," and processes, such as the creation of a data agency to oversee the execution of data and privacy laws and prevent the inward or outward transfer of personal information outside the specified jurisdictions, are required [11].

This would ensure African-centric e-Health privacy protections, thereby accelerating the growth and adoption of e-Health projects that address Africa's demand for affordable and accessible healthcare.

D. Issues and challenges in e-Health implementation in Africa

However, the e-Health system has its own set of challenges that must be thoroughly discussed in this study for proper mitigating strategies to be implemented. The first challenge of eHealth explained by [19] is Infrastructural and Resources Barriers to e-Health. According to the studies, implementing eHealth successfully in a developing country require the deployment of modern infrastructure and technology. The research identified hardware and software, Internet and IT professionals as the major components which can create infrastructure barriers implementing eHealth.

Internet, Software and hardware, and IT professionals

Since the internet was introduced, it has proven to be more useful in supporting the search for information which most health professionals depend on in making effective decisions these days [20]. In their research, [21] concluded that poor internet services and required skills affect the implementation and performance of eHealth in many aspects. It was explained that if one lacks the skills to surf the internet, it is difficult to identify biased data or understand which available data is meant for healthcare delivery. Furthermore, some health workers lack the reading skills required to extract health-related data from the internet [22]. Again, the speed of internet service in developing countries is mostly poor, and accessing immediately needed information for a particular patient’s intervention is a challenge. Other technological resources that can help to extract relevant health information online to assist in healthcare delivery are not readily available in most developing countries [23]. Proper eHealth implementation requires the use of needful hardware and software technologies operating over a network to allow communication and sharing of resources. The hardware would include computers and accessories, smart mobile phones with internet capabilities, servers, switches, and many others for the

implementation of eHealth systems. The eHealth packages are mostly developed applications with health populated databases and internet sync technologies. One omission mostly committed during implementation is engaging the opinions of health professionals in the planning, development, interface designing, and customization of eHealth intervention software to make it more user-friendly for easy adoption [24]. Even when successfully implemented, [25] believe the complex nature of an interface design and using the eHealth system is deterring a lot of health professionals from attempting to even use the eHealth systems to support daily activities. Meanwhile, [18] concluded health workers in developing countries have made numerous submissions on how complex the content and language used in some eHealth systems are to understand and how their functionalities also do not conform to their daily practices at work. As a result, [26] indicated in their research that the IT workforce in the developing countries for most health organizations require extensive training as they lack the competent computer skills and ability to learn them due to limited resources.

Most eHealth projects fail, according to [27], because health organizations, in general, lack IT professionals to maintain and sustain the e-Health system. Because developing countries in general lack advanced IT training, resources allocated for eHealth are always squandered without yielding any benefits from their implementation. As a result, [28] concluded that training programs for all health IT professionals should be conducted regularly to promote the use of eHealth systems. When more health workers are involved in the training program, the capacity of IT health professionals will increase, as health professionals will become more knowledgeable about the use of eHealth applications and the internet.

Policies and Strategies to govern the usage of eHealth

Policy is defined by [29] as a collective statement, directive, or law that governs and maintains the eHealth cycle. The policy may be implemented as part of other policies such as general health policies or e-governance policies and many others. Proper policy implementation governs how the system must be used or what rights one has concerning the system. The policies are mostly planned and executed by the Ministry of Health. The problem is that policy objectives differ across countries, so there is no consistency in policy formulation. Another major challenge is that there is no common goal for the various eHealth policies, and it is impossible to conclude the policy impact on real-life practices [30]. In most developing countries the system lacks the expertise to advise management on which policies should be implemented.

E. Security and Privacy

One major challenge with e-health is a concern for patients' data privacy and data protection. The e-health system requires sharing and transmission of volume data from one healthcare facility to another. Patients' information has always been regarded as highly sensitive, necessitating safeguards against unauthorized access or use. As a patient, one becomes more vulnerable in the face of pressure and can share any sensitive information including job sensitive information or personal data such as house address which could be used by an adversary health worker. Patients may not be able to control or decide on what their data might be used for once a party gets access to it [31]. According to [32], it is even more dangerous when health records are deployed over networks with the internet as the backbone. Patients' data are made available and accessible anywhere to medical professionals such as physicians, nurses, and others who might have less knowledge about ensuring privacy, confidentiality, and protection of user data. e-Health services might comprise of patients' charts, reports among many other records that are very vital for quality of care delivery. It is more likely that a patient's conditions can easily be made known to an undesired person if not properly handled. The bigger picture of the problem involves hackers, who could cause a slew of issues, including network hijacking and widespread spying on patient records if proper security measures are not implemented. It should be emphasized that unauthorized access and misuse of user data can result in criminal charges and penalties, as implemented user data privacy policies and laws ensure that users' data is protected at all times [33]–[35]. In their article, [36] also explained that sixty state-level laws have been implemented which concerns healthcare records. eHealth implementation necessitates two distinct levels of security, thereby protecting the e-Health system from external attacks such as hackers and preventing user data from being misused by health professionals. This was explained and categorized by [36] as organizational and systemic threats respectively. Different threats that a patient is likely to face under obscurity are categorized into health data integrity and privacy, medical identity theft, and security breaches [37]. According to [38], a patient's trust is everything to them, and knowing how vulnerable they are after disclosing sensitive information to health professionals is likely to discourage them from using the eHealth system. Patient safety must be prioritized, and under the Health Insurance Portability and Accountability Act (HIPAA), all health data pertaining to patients must be encrypted if transmitted over an open network.

Furthermore, to improve the performance of e-Health applications such as diagnoses systems to support effective care delivery, a large dataset on patients may be required for training and testing for performance, which may contradict the goal of the user data preservation policy.

To address this security and privacy issue, the health care industry must implement eHealth solutions with proper policies, guidelines, and regulations that adhere to HIPAA, state regulations, and industry best practices standards.

III. PROPOSED PRIVACY BY DESIGN FRAMEWORK FOR E-HEALTH

Most research conducted has focused on issues and challenges of e-health adoption in Africa. In Africa, little research has been conducted in the area of privacy by design for eHealth as identified in Section II. Security and privacy solutions have been proposed over the period to address security and privacy challenges when adopting technology in an organization. Unfortunately, the majority of e-health security and privacy solutions proposed in Africa have focused on general security and privacy principles. As mentioned in Section II, it is critical to develop and enforce security and privacy policies to guide the use of e-health systems. Also, because e-

Health systems rely on a network, particularly the internet, to provide services to users, it is critical to identify and analyze threats that may impede their use.

To come up with a better solution, we looked into the challenges, practices, and mechanisms that would improve e-Health security and privacy. The proposed framework is designed to provide data security and privacy in a health organization. It is aimed at securing, detecting security and privacy incidents, and collecting potential digital evidence in e-Health Platforms. Well-known implementation practices are employed to establish a dynamic and effective framework when implemented in small or large health organizations. The proposed framework enhances the existing privacy by design procedures for eHealth adoption. It allows the introduction of new technologies by the organization when adopted.

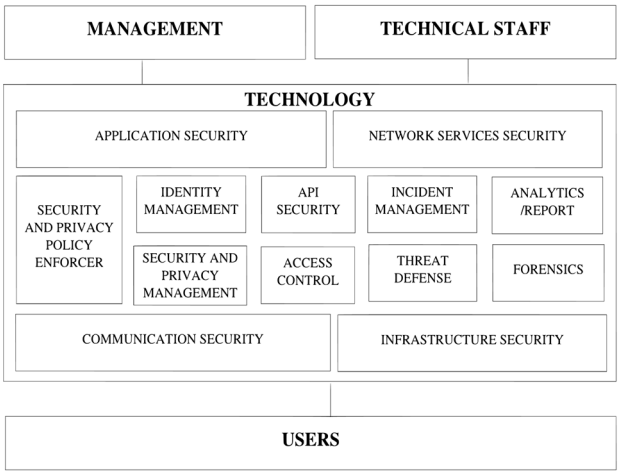

Fig. 1. Proposed privacy by design framework for eHealth

A. Proposed Privacy by Design Framework for eHealth

The proposed framework is illustrated in Fig. 1. The framework is based on four components: Management, People, Technology, and Users. The four components are discussed below:

- **Users:** Users include patients and staff who can access the organization's resources. All eligible users should be authorized to access resources when connected to the organization's network or services. Service level agreement (SLA) should be implemented to allow legal monitoring of users' activities especially staff to enable the gathering of digital evidence.
- **Management:** Management ensures the development and implementation of security and privacy controls. It certifies security and privacy programs and policies for an organization. Management oversees and monitors all approved security policies. To provide effective implementation of privacy by design in a health organization, risk management, and assessment are to be performed. Top management oversees the governance of users, technical people, and technology. Legal and regulatory requirements are to be established in addition to other policies in the organization.
- **Technical Staff:** A health organization's IT department provides technical personnel to manage and provide applications and services to users. They are responsible for enforcing the organization's approved policies. They are to ensure privacy by design strategies when applications and devices are being developed or purchased for the health organization. The application, product, and process requirements must all be satisfied. Every deficiency must be detected and addressed regarding application, product, and processes. To ensure privacy and security continuity, applications, products and processes need to be proactively evaluated and audited.
- **Technology:** This domain consists of technologies and mechanisms that ensure security and privacy in an organization. The technologies consist of policy database, access control, security, and privacy policy enforcer, identity management, security and privacy management, API security, incident management, threat defense, forensics, and analytics/report. The technology domain also ensures there is an application, network services, communication, and infrastructure security in the organization.

  Well-defined policies to handle security and privacy will be stored in the policy database. The security and privacy policy enforcer will ensure that users comply with the organization's security and privacy policies. It will also prevent any privacy-invading activities that may occur. Implementing and enforcing policies should guide users by creating an awareness of their actions and activities. Well-defined policy implementation will help to foster a privacy culture [39]. Properly defined policies set requirements for security and privacy to be incorporated into processes and the development and acquisition of applications and products. Defined policies should also allow health organizations to collect and analyze digital evidence, allowing them to undertake investigations based on the information gathered. There should be periodic updates or audits of these policies to ensure effective privacy inclusion in the organization. Access to resources is to be monitored and recorded to comply with the organization's policies. User access to resources should be controlled and managed by access control, security and privacy management, and identity management.

  To manage organizational users and devices, the identity management component will be used. This component identifies various users to ensure proper management and monitoring. Identity management complies with the organization's policies and ensures that users follow them.

  API Security ensures the identification and prevention of API vulnerabilities in applications that will be utilized in the organization. Authentication and authorization mechanisms will be utilized to permit access to required resources or data while also preventing attacks.

The forensic component ensures the collection of forensic information and logs from resources, identity manager, threat defense, and API Security components. Digital evidence collected will be preserved using crypto operations such as hashing and encryption.

By collecting threat data feeds, the threat defense component will guarantee the preparation, identification, and prevention of cyber threats. This component ensures the acquisition of threat actors' techniques and procedures. Effective implementation promotes the trust of users when data and resources are protected from threats.

Security and Privacy management employ constant monitoring to ensure the security and privacy of resources and data in the organization. In addition to access control, it also allows the rejection of unauthorized access to resources and data.

All security and privacy incidents that potentially result in the loss or disruption of the organization's operations, services, or functions are identified, analyzed, and corrected by the Incident Management Component.

The analytics/reporting component generates reports that analyze and assess the organization's security and privacy strategies or processes implemented. It also enables the organization to make evidence-based and analytics-driven security and privacy decisions.

When it comes to implementing e-health, the proposed framework provides the necessary guidelines. Existing and new security and privacy solutions can be integrated to improve e-health platform security and privacy.

B. Discussion

The proposed framework aims to address the need for developing countries such as Africa to adopt privacy by design when implementing e-health. It embeds security, privacy, and forensics to create an environment that can foster the growth of e-health. African countries that want to implement e-health services can adopt the framework. It also enables researchers and developers to create enhanced security and privacy solutions capable of protecting the e-health platform from potential threats, vulnerabilities, and privacy concerns.

Even though the framework can provide the standard platform when implementing e-health, the framework's capabilities must be enhanced to provide the best solution. Because internet connectivity is a major issue in most African countries, it is critical to assess the problem and propose a solution to address it. A more thorough assessment of cloud, Bring Your Own Device (BYOD) and Internet of Things (IoT) security will be required in the future. As data feeds can be expensive, open-source data feeds and solutions, in addition to internally generated data feeds, can be used to support the environment.

IV. CONCLUSION

As healthcare is important to every country, it is essential to improve its operation. The introduction of technology into health care practices to provide better services is known as eHealth. This adoption by countries poses privacy and security challenges. As a result, this study identifies the privacy and security challenges that African countries face when adopting e-health, as well as the need for African countries to incorporate privacy by design procedures. By evaluating the challenges, procedures, and mechanisms required when adopting e-health to improve privacy and security, privacy by design framework for e-health was proposed. Because e-health systems are vulnerable to security and privacy threats, the adoption and implementation of this framework will significantly improve the health sector's privacy and security posture. The proposed framework considers users, technical staff, technology, and management as key components when implementing privacy-by-design into e-health. To detect and collect privacy and security incidents, the framework employs technologies and security solutions such as API security, forensics, and threat defense. To protect e-health systems, it adopts privacy and security policies that are implemented and enforced. The proposed framework will also serve as a trusted platform for the delivery of improved health services.

REFERENCES

[1] E. A. Teviu *et al.*, "Improving medical records filing in a municipal hospital in Ghana.," *Ghana Med. J.*, vol. 46, no. 3, 2012.

[2] M. Acquah-Swanzy, "Evaluating electronic health record systems in Ghana: the case of Effia Nkwanta regional hospital," UiT Norges arktiske universitet, 2015.

[3] R. Wynn, T. Meum, G. Wangensteen, and K. S. Soleng, "How does nursing staff perceive the use of electronic handover reports? A questionnaire-based study," *Int. J. Telemed. Appl.*, 2011, doi: 10.1155/2011/505426.

[4] I. D. Norman, M. K. Aikins, and F. N. Binka, "Ethics and electronic health information technology: challenges for evidence-based medicine and the physician-patient relationship.," *Ghana medical journal*, vol. 45, no. 3. 2011.

[5] S. YUSIF and J. SOAR, "Preparedness for e-Health in developing countries: the case of Ghana," *J. Health Inform. Dev. Ctries.*, vol. 8, no. 2, 2014.

[6] S. Z. Khan, Z. Shahid, K. Hedstrom, and A. Andersson, "Hopes and fears in implementation of electronic health records in Bangladesh," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 54, no. 1, 2012, doi: 10.1002/j.1681-4835.2012.tb00387.x.

[7] S. O. Oyeyemi and R. Wynn, "Giving cell phones to pregnant women and improving services may increase primary health facility utilization: A case-control study of a Nigerian project," *Reprod. Health*, vol. 11, no. 1, 2014, doi: 10.1186/1742-4755-11-8.

[8] S. Arora, J. Yttri, and W. Nilsen, "Privacy and security in mobile health (mHealth) research," *Alcohol Res. Curr. Rev.*, vol. 36, no. 1, p. 143, 2014.

[9] A. Cavoukian and others, "Privacy by design: The 7 foundational principles," *Inf. Priv. Comm. Ontario, Canada*, vol. 5, p. 12, 2009.

[10] G. Eysenbach, "What is e-health?," *J. Med. Internet Res.*, vol. 3, no. 2, p. e20, 2001.

[11] M. Namara, D. Wilkinson, B. M. Lowens, B. P. Knijnenburg, R. Orji, and R. L. Sekou, "Cross-cultural perspectives on eHealth privacy in Africa," in *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, 2018, pp. 1–11.

[12] K. C. Montgomery, J. Chester, and K. Kopp, "Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection," *Cent. Digit. Democr. Rep.*, 2016.

[13] A. B. Makulilo, "Privacy and data protection in Africa: a state of the art," *Int. Data Priv. Law*, vol. 2, no. 3, pp. 163–178, 2012.

[14] A. B. Makulilo, "The context of data privacy in africa," in *African Data Privacy Laws*, Springer, 2016, pp. 3–23.

[15] B. Townsend, "mHealth regulation impact assessment Africa," *Mob. Dev. mHealth*, 2015.

[16] L. A. Bygrave, "Privacy and data protection in an international perspective," *Scand. Stud. Law*, vol. 56, no. 8, pp. 165–200, 2010.

[17] A. B. Makulilo, "Myth and reality of harmonisation of data privacy policies in Africa," *Comput. Law Secur. Rev.*, vol. 31, no. 1, pp. 78–89, 2015.

[18] A. Chetley *et al.*, "Improving health, connecting people: the role of ICTs in the health sector of developing countries A framework paper," *Infodev*, no. 7, 2006.

[19] Q. A. Qureshi *et al.*, "Infrastructural barriers to e-health implementation in developing countries," *Eur. J. Sustain. Dev.*, vol. 2, no. 1, p. 163, 2013.

[20] F. Griffiths, A. Lindenmeyer, J. Powell, P. Lowe, and M. Thorogood, "Why are health care interventions delivered over the internet? A systematic review of the published literature," *Journal of Medical Internet Research*, vol. 8, no. 2. 2006, doi: 10.2196/jmir.8.2.e10.

[21] A. Muzaffar, A. Malik, N. M. Larik, and S. A. Khan, "Use of information technology by practising clinicians in Pakistan: a questionnaire survey," *J. Health Inform. Dev. Ctries.*, vol. 2, no. 2, 2008.

[22] T. P. Hogan and C. L. Palmer, "Information preferences and practices among people living with HIV/AIDS: Results from a nationwide survey," *Journal of the Medical Library Association*, vol. 93, no. 4. 2005.

[23] M. Benigeri and P. Pluye, "Shortcomings of health information on the Internet," *Health Promot. Int.*, vol. 18, no. 4, pp. 381–386, 2003.

[24] S. Khoja, R. E. Scott, A. L. Casebeer, M. Mohsin, A. F. M. Ishaq, and S. Gilani, "e-Health readiness assessment tools for healthcare institutions in developing countries," *Telemed. e-Health*, vol. 13, no. 4, 2007, doi: 10.1089/tmj.2006.0064.

[25] R. A. Hughes, "Clinical practice in a computer world: Considering the issues," *Journal of Advanced Nursing*, vol. 42, no. 4. 2003, doi: 10.1046/j.1365-2648.2003.02625.x.

[26] H. Kimaro and J. Nhampossa, "The challenges of sustainability of health information systems in developing countries: comparative case studies of Mozambique and Tanzania," *J. Health Inform. Dev. Ctries.*, vol. 1, no. 1, 2004.

[27] G. M. Kundi, "E-Business in Pakistan: Opportunities and Threats, Lap-Lambert." Academic Publishing, Germany, 2010.

[28] M. S. Qazi and M. Ali, "Pakistan's health management information system: Health managers' perspectives," *J. Pak. Med. Assoc.*, vol. 59, no. 1, 2009.

[29] R. E. Scott, M. Faruq, U. Chowdhury, and S. Varghese, "Telehealth policy: Looking for global complementarity," *J. Telemed. Telecare*, vol. 8, no. SUPPL.3, 2002, doi: 10.1258/13576330260440871.

[30] P. Hämäläinen, P. Doupi, and H. Hyppönen, "The European eHealth policy and deployment situation by the end of 2006," *Deliverable*, vol. 2, pp. 1–187, 2007.

[31] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, 2015, pp. 1310–1321.

[32] J. R. Shah, M. B. Murtaza, and E. Opara, "Electronic Health Records: Challenges and Opportunities," *J. Int. Technol. Inf. Manag.*, vol. 23, no. 3/4, 2014.

[33] A. Silde and O. Angelopoulou, "A digital forensics profiling methodology for the cyberstalker," 2014, doi: 10.1109/INCoS.2014.118.

[34] B. M. Gaff, H. E. Sussman, and J. Geetter, "Privacy and big data," *Computer (Long. Beach. Calif).*, vol. 47, no. 6, pp. 7–9, 2014.

[35] C. Tankard, "What the GDPR means for businesses," *Netw. Secur.*, vol. 2016, no. 6, 2016, doi: 10.1016/S1353-4858(16)30056-3.

[36] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," *Int. J. Internet Enterp. Manag.*, vol. 6, no. 4, 2010, doi: 10.1504/ijiem.2010.035624.

[37] I. Clarke, T. Flaherty, S. Hollis, and M. Tomallo, "Consumer privacy issues associated with the use of electronic health records.," *Ahcmj*, vol. 5, no. 2, 2009.

[38] R. Kam, "Top 3 issues facing patient privacy," *Gov. Heal. IT. Retrieved from http//www. govhealthit. com/news/top-3-issues-facing-patient-privacy*, 2012.

[39] A. Cavoukian, "Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices," *Inf. Priv. Comm. Ontario, Canada*, no. December, 2012.