Electronic Health Record Systems and Cyber-Security Challenges

Onuiri Ernest E., Idowu Sunday A., Komolafe Oyindolapo
Department of Computer Science
Babcock University
Ilishan-Remo, Ogun State, Nigeria

Abstract— Research findings have revealed that our world today is greatly influenced by the digital cyberspace and the corresponding information flow resulting in huge societal and economic impacts. Cyberspace offers an imagined place or notional realm in which electronic information exists or is exchanged. The explosion of the Internet has placed increasing demands on businesses, industries, commerce, government, education, entertainment and health, thereby creating vulnerabilities within the cyberspace and increasing criminal, hostile actions and potential threats. In the health sector, application of Electronic Healthcare Records (EHRs) provide a means to sustain patient safety and care while allowing better efficiency in the exchange of information, but with the risk of privacy violation and identity theft. In view of the foregoing, developing economies especially in sub-Saharan Africa, seem reluctant to key into this aspect of healthcare management, which has harmed greatly certain initiatives to implement and sustain healthcare schemes. Whereas consensus efforts have been made to stem the tide, such as the exploration of threat combative mechanisms such as cryptography; a technique that can maintain authentication, integrity, availability, confidentiality, identification and privacy of data by encryption and decryption, the cyber-security war cannot be said to have been won. Other security means involve the integration of privacy settings into hardware and the use of biometrics. This research focuses on the various challenges that exist in today's cyberspace, especially the impact observed in the medical and healthcare field, with respect to securing information and harnessing steps, that could be implemented to mitigate and if possible, totally eradicate the causes and effects, and consequently suggest action steps which developing economies can adopt in implementing robust EHR systems.

***Index Terms*— Cyberspace, Electronic Health Record, Security**

I. Introduction

Advancement in technology, a great leap in the 21st century has been defined by an increase in information and communication technology infrastructure. Our world today is greatly influenced by the digital cyberspace and the information within it, resulting in a huge impact on businesses, education and overall way of life. Cyberspace offers an imagined place or notional realm in which electronic information exists or is exchanged. It refers to an imagined world of virtual reality [1]. Cyberspace which in recent times, is used synonymously with the Internet or world wide web is a computer jargon first adopted by American writer, William Gibson in a science fiction novel 'Neuromancer' in 1984 [1].

With the passage of time, information generated increases as more activities are carried out by individuals, organizations and nations, leading to a ripple effect on the risks involved in security, management and accessibility of data. Explosion of the Internet has placed increasing strain on businesses in industry, commerce, government, education, entertainment and health. Consequently, the cyberspace has created more ways for criminal, hostile actions and potential threats to the owners of the information processed and stored in it [2].

Over the years, technology has experienced infiltrations in its security such as integration of false data or harmful programs into information systems, loss of valuable data or programs from a system due to theft and overall control takeover of a system's operation and performance. These breaches in security are usually carried out by hackers as a way of gratifying their personal agenda, criminals who use it to advance their own causes, commercial organizations as instruments to neutralize competitors or terrorists whose attacks can spread over a wide geographical range, ultimately creating similar effects regardless of the perpetrator of the crime [2]. Aside from these deliberate attacks, information systems operating in the cyberspace can also cause damages as a result of software and hardware failures, and protection against this is coined "cyberspace safety".

The issue of cyber security especially when dealing with information, cannot be over emphasized as is cited in a case involving the Defence Department of the United States, losing an average of 24,000 sensitive Pentagon files in 2011 as a result of a huge cyber-attack [3, 4]. It is quiet alarming that one of the highest-priority sectors of the American government, which consumes a great deal of resource such as finance (over 500 billion dollars a year), and houses some of the most advanced technology systems for security can fall prey to hackers operating in the cyberspace. Swiss companies who have been a major target, have started to put in place steps to alleviate the impact of threats to the business, as total eradication could well be a dream that will never come to reality [5].

Medical or health information consist of medical history reports, patient discharge summaries and drug information, which form an individual's Protected Health Information (PHI) [6]. Improvement in healthcare

organizations include the application of Electronic Healthcare Records (EHRs), to sustain patient safety and care while allowing better efficiency in the exchange of information. In addition, certain on-line services like Google Health and Microsoft Health Vault allow individuals the easy access to their records online, but with the risk of privacy violation and identity theft (Security and privacy of electronic medical records). Sadly, most of these services are outsourced by hospitals and medical offices, owning to the ease of information transfer over the Internet. Patients can bear huge financial consequences and emotional harm in the event of unlawful disclosure of their billing data and PHI. Instances of privacy breaches with effects on the confidentiality and integrity of medical information include but not limited to:

- VIP record snooping: This entails the disclosure of a celebrity's medical records, such as the case which occurred when an employee of the University of California, Los Angeles (UCLA) Medical Centre, disclosed information regards an actress, Farah Fawcett's cancer treatment records to the papers.
- Financial identity theft: In this case, a patient's record is stolen for financial gain. An admissions clerk at the Baptist Health Medical Centre in Little Rock, United States, faced accusation of stealing about 1,800 patient records to by Wal-Mart gift cards.
- Medical identity theft: This suggests using patient data to acquire treatment claims, medical treatment or purchase drugs. A cousin of a front desk clerk at a Florida medical clinic received $2.8 million for false Medicare claims by using downloaded medical information of more than 1,100 their patients.
- Co-worker, family member and neighbour snooping: A CNN reporter Elizabeth Cohen used a fellow colleague, Gary Tuchman's birth and social security number to access 18 months of his medical records [7].

Securing the availability, confidentiality and integrity of a patient's medical and health information, requires the implementation of robust and reliable clinical applications as well as Information Technology (IT) infrastructure. With the number of healthcare personnel such as nurses, physicians, technicians, requiring access, application-layer security needs to be monitored in conjunction with IT systems, employee communications and policy violations. The IT security team has the responsibility of promoting information security information and event management (SIEM) by providing insight to the vulnerabilities that may exist in the system or network, owing to both internal and external threats. The need to assess threats, in accordance with the organizational mission and operating model becomes utmost in understanding the effects which vary significantly across the government and industry sectors [8].

There are three categories of people with major interest in medical and health information with the collective responsibility of ensuring its security.

- Private individuals: Authentication is very important in ensuring security. Biometrics is a way of measuring, analysing and using physiological and behavioural traits to identify an individual, and could be used by patients as a means of accessing their records. It is more effective than the use of passwords or PIN (Personal identification number) codes, because access is still possible in instances when the patient too sick and incapable of entering data or information. This system would however require adequate training especially for children and the aged [9].
- Government: A report written by Rosenzweig [10] on a workshop jointly conducted by the American Bar Association Standing Committee on law and National security and the National Strategy Forum, addresses certain issues regarding the national security threats in cyberspace. Not all threats to national security have its roots in cyberspace and not all cyber security threats do become national.

In 1986, the Computer Fraud and Abuse Act (CFAA) was passed, which legalised a number of computer crimes. Government regulations have been passed in several countries in a bid to ensure adequate protection of medical and health information across the globe. A few of these healthcare regulations include:

- The Health Insurance Portability and Accountability Act (HIPAA) in America which states that healthcare providers must employ suitable systems and practices in the management and disclosure of PHI.
- The Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery and Reinvestment Act (ARRA). This act builds on HIPAA by infusing other regulations on the confidentiality of EHRs.
- FTC Red Flags Rule: The Federal Trade Commission (FTC) mandates healthcare providers, to employ practices and systems that fight against identity theft.
- Data Protection Act: Effective in the United Kingdom (UK), this act covers the protection and regulates the right of accessibility of data.
    - Organizations also exist like the European Network and Information Security Agency whose role is to enhance the cyber security preventive work and capability of the European Union (EU) and its member states.

- Healthcare organizations: Protection of health information is for an aspect of risk management for hospital, medical and health centres. The first stage of this is the formation of a security committee to oversee the entire organization, consisting of all medical staff, legal representatives and the team in charge of information technology [11], though some healthcare centres may outsource securing their data to an external organization. The security committee has the responsibility of carrying out the following actions:
- Risk analysis: by identifying the technology used for the processing, storage and transfer of information within the health care system coupled by a thorough analysis of ePHI transmission and clinical communication to reduce information transfer to the barest minimum and ensure conformity with the government laws.
- Risk management: Policies should be established to manage risks in event of information security breaches. Protective techniques and procedures could be implemented such as the need for authentication during request for access, monitoring of all access logs, varying the level of access with the different types of users, use of more secure software, improved access controls, encrypted communication and use of encrypted files and data [2].
- Implementation of policies and procedures: This includes proper training of staff, establishing the various levels of responsibilities. An example of such is for physicians and nurses to share electronic protected health information (ePHI) with each other only via a secure application or platform that is downloaded onto their means of communication, and assign an individual to track those communications to ensure maximum security [11].
- Risk Monitoring: The security of information within the organization needs to be monitored over time. Changes and advancement in technology and health care would expose information to more risks and therefore require modifications to policies and procedures.

II. Problem Statement

Medical and health information is tremendously sensitive and volatile in nature. Security is therefore very important as any interference or compromise, may lead to issues such as erroneous diagnosis or treatment, and in extreme cases, death. Owners and users of medical information expect confidentiality, an act of secrecy and integrity by ensuring the information is honest and true. The protection of privacy by ensuring confidentiality, integrity and availability of patient information is not only considered an advancement in technology but also a legal requirement in many countries today [7]. Technologies such as EHRs and on-line personal health services have improved the dissemination of information on one hand, but also raised challenges of security on the other hand.

The nature of cyberspace threats usually take the form of being broad, embedded and diverse [10]. Threats are broad because cyberspace is extensively wide, embedded because they arise from loop holes in the complex software and sophisticated hardware, both substantially constitute the cyberspace, and hence, can never be destroyed. Lastly, these threats are diverse, due to the huge number and different forms of "actors" ranging from individuals to terrorist groups, with different agenda for breaching cyber security. All these reflect the need in a dynamic healthcare environment to monitor information by employing laws and policies, for securing all aspects of electronic communication without compromise [11].

III. AIM and Objectives

In view of the foregoing, this research paper aims to explore the various challenges that exist in today's cyberspace especially the impact observed in the medical and health care field with respect to securing information as well as harness steps that can be implemented to mitigate and where possible, totally eradicate the causes and effects that leads to the adoption and implementation of EHR systems in developing economies. Hence the objectives are to:

- Investigate the nature of cyberspace threats that result in security challenges and identify the contents of medical or health information, the methods of information exchange, storage and access that occur within the cyberspace.
- Highlight methods being incorporated to detect, mitigate and avoid the threats identified in the first objective, by evaluating and converging actions carried out by the individuals, private organizations and the government, on both local and international levels in information management of the medical care field.
- To identify proactive measures that will catalyse the implementation and sustenance of EHR systems in developing economies like Nigeria that will serve as the platform to successfully support health policies such as the health insurance scheme and the likes.

IV. Review of Related Works

This section entails brief discourses of existing related works.

A. The e-Logistics of Securing Distributed Medical Data

The research conducted by Snyder and Weaver [12], both from the department of computer science, in the University of Virginia, focused on the performance of four candidate algorithms operating in the .NET environment, using a hospital's radiology department to predict the impact of encryption on workflow.

When HIPAA was signed into law by the United States Congress in 1996, a process was initiated to ensure that all healthcare data accessed or transmitted over communications systems such as the Internet are encrypted. However, the privacy and security rules, effective from April 24, 2004 provided the means of ensuring patient privacy by regulating the manner in which medical information is managed, stored, used and disclosed by doctors, hospitals, healthcare plans, insurance companies and other interested parties. Owing to the law, hospital records are periodically audited to ensure that encryption requirements for data security, are of the stipulated standard as information dealing over an open network, like the Internet are mandated to be encrypted, though encryption is optional when operating within a closed network.

The University of Virginia Medical Centre, the hospital under this study, houses electronic patient records encompassing diagnostic imagery acquired by the department of radiology, which conducts over 380,000 examinations and generates around 9TB(Terabyte) of data on an annual basis (statistics as at time of research). The main aim of the research project was to determine the best suited encryption method to ensure a smooth workflow within the hospital. Of the various encryption methods available, the four of central focus while conducting their research, weighing security opposed to speed when in use in a healthcare environment are:

- The Data Encryption Standard (DES). This is a legacy type of algorithm for hardware.
- Triple – DES. A more secure, though slower step-up from DES.
- The Advanced Encryption Standard (AES). Better and much faster than DES.
- RSA: best known of the four, though performance is slower.

The RSA which is best used for small quantity of data, displayed slower decryption, at rates 100 times lower than the other three techniques, although both the encoding and decoding are alike in all four methods. DES is the fastest and also produces the highest throughput while AES is the slowest of the four.

A model was then created of the University of Virginia's Department of Radiology's Picture Archive and Communication System (PACS) in other to conduct throughput assessments and identify possible bottleneck in its clinical procedures. Other parts of the department incorporated into the model include, the Hospital Information System (HIS), Radiology Information System (RIS) and Digital imaging.

Results show that encryption does not pose as a bottleneck neither does it bring about changes in the bottleneck resource, but it does decrease the throughput of the bottleneck. For example, the resource bottleneck could permit an average of 62 patients in 24 hours, for a single doctor without encryption. This number is reduced by 5% to approximately 59 patients for the same time duration, when encryption is employed and could go further to a 7% reduction, in cases where all documents need to be entered before proceeding to the next patient. Although the model reflects a 5 to 7% decrease in throughput when encryption is exercised, the effect is marginal and can be negated by increasing efficiency in other aspects.

The use of AES with the 256-bit keys is recommended for use since it produced a throughput of 6.81MB/s with a 3 GHz Pentium 4. The research therefore proved that the allowable data security according to HIPAA will not disrupt the workflow of the radiology department in any radical manner.

B. Privacy Challenges for Wireless Medical Devices

This research by Lagesse [13], from Cyberspace Sciences and Information Intelligence Research, Computational Sciences and Engineering, Oak Ridge National Laboratory, highlights the need for wireless medical devices to be protected to ensure security. With the increase of wireless technology, especially the use in medical devices and services, exposure of patient information also rises. Earlier work done tackled the privacy of information from devices, even with encrypted information, which exposed the need for the devices themselves to be protected, most especially in implantable medical devices. Standard methods of enhancing privacy such as encryption, k-anonymity or mixes are not appropriate for a lot of medical devices, and these were explained. In the case of encryption, information sent between components can still be retrieved from traffic analysis, by examining the traffic patterns to reveal device types.

K-anonymity is a technique by which a data set is "anonymized" to the point that the identity of an entry can only be narrowed to a set of k-individuals. This technique, which has been used for static databases, can be used to transmit information in medical devices and has the capability of covering the traffic as well as extend battery-life which is a downside of encryption. As of now many do not view medical device privacy, as important but this is likely to change as more devices go wireless. Privacy can be achieved by hard-coding privacy settings into the implantable device.

C. Securing the Communication of Medical Information Using Local Biometric Authentication and Commercial Wireless Links

In 2011, Ivanov and Baras [9], both from the University of Maryland USA, in conjunction with Yu P., from the United States Army Research laboratory in Adelphi, discovered a means of securing medical information using local biometric authentication and commercial wireless links.

A portable, wireless device was used to transfer medical information to a remote server providing ways to secure the link between the patient and the portable device, and in turn securing the link between the portable device and the network. The user is authenticated using their biometric information (fingerprinting), authenticating the device to the network at the physical layer and reinforcing the security of the wireless link via a key exchange method. The issue of securing data while maintaining confidentiality arises, when wireless sensor networks are used in healthcare systems. In addition, using biometrics can cause a whole range of challenges, because there are a number of low-cost and small sized systems that are easily commercially available, and the biometric information could be readily captured and used to produce an artificial one, without the knowledge of the user. This compromise could be more catastrophic than that of using a password, as changes to an individual's biometric information is not easily achievable except by surgery. In addition, the breach may be more difficult to detect.

Hence, the researchers therefore produced a portable device in sole possession of the user, to store the biometric information instead of the storage on a computer or server. The device is locked using special hardware, which offers a higher security level and fingerprinting was used as the biometric authentication. Confidentiality of the biometric information was attained by means of a Trusted Platform Module (TPM), specified by the Trusted Computing Group (TCG). TPM, according to Ivanov et al [9], is a 'locked-down' architecture that protects the integrity and confidentiality of the data, with hardware support using cryptographic keys built into the hardware. The TPM was incorporated into the device and encrypted with keys managed by it. The biometric information is stored in the smart chip of a smart card which as a property of the user, can be inserted into the portable device when local authentication is required.

Furthermore, the second level of authentication is required for communication from the device to a network access point or remote server, by utilising physical layer techniques that exploit the variation of radio frequency of different devices. The three usual methods of device-to-network authentication are: handshaking protocols, an example of such is Kerberos, digital signatures and certificates (example, X509) and symmetric authentication like the use of MACs (Media Access Control). The researchers combined their method of artificially embedding a stealthy fingerprint tag into the modulation waveforms communicated between the two parties with the current security methods to increase the security of the device, incorporating the Markov model to direct the key exchange between two parties. The Markov chain is a random process, where future occurrences depends on the present and is not at all influenced by the past. The portable device and the network access point, are paired using a shared secret key and as long as the two parties share the same model, the keys can be exchanged and replaced while being synchronized.

Consequently, the network access point ensures that the user of the portable device is legitimate and does not process any message until a successful local biometric authentication, which is important, so that no medical information is transferred until a valid fingertip is used. This method of authentication could also be used by nurses and doctors to authenticate users to their medical storage, thereby monitoring accessibility to data and electronic patient records. In this system the patient not only enters, but can also maintain and control the transfer of their unique data. Further work involves employing the method in other sectors such as finance and mobile commerce, and study into development of high-level applications that can connect the patients directly with the healthcare systems.

D. Ensuring Patients Privacy in Cyberspace

This study was conducted by Seth Crouch [11], a director of ambulatory services at the Covenant Medical Group in Lubbock, Texas with contributions from Terry Edwards, chief executive officer of PerfectServe in Knoxville, Tennessee. In Crouch's opinion, the focus of securing ePHI rests on the organization forming a security committee with members such as the medical, legal and Information Technology (IT), staff carrying out four essential steps:

- Conduct a formal risk analysis to assess and identify the technology needed for communication, bearing in mind adherence to laws and regulations governing the transfer of electronic data.
- Establish an appropriate risk management strategy, by the formation of policies and procedures to ensure security of data during transmission and storage as well as compliance with laws and regulations.
- Rolling out these policies and procedures and adequate training of healthcare staff especially those handling medical data.
- Monitoring of risk and challenges to ensure security standards are always met.

V. ELECTRONIC HEALTH RECORD (EHR)

EHR is defined by Lakovidis [14] as digitally stored healthcare information about an individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times. EHRs can be explained as being a repository of an individual's lifetime healthcare and status information. The information in the EHRs contains treatments, observations, laboratory tests, diagnostic imaging reports, therapies, prescriptions, allergies and medical history in general. EHRs provide enablement to manage health information, using modern information techniques that are impossible to apply to paper record keeping.

Features of EHR include:

i. Increased patient safety: EHRs provide universal availability of full healthcare services to all citizens and access to quality healthcare services. It provides information about a patient's family, medical and career history. Hence, in case of chronic or critical conditions, quick treatment is ensured.
ii. Reduced cost: the easy retrieval and transfer of patient's records reduces cost of duplicating tests and prescriptions.
iii. Security and fraud detection: the system ensures data protection, data accuracy and integrity.
iv. Improved productivity: EHRs help to reduce errors and improve productivity of the healthcare sector.

Figure 1 shows a flowchart of the processes and stages involved in collecting data for EHR. The flowchart shows the sequence of activities that are involved to have a robust EHR in Nigeria. Figure 2 shows the data flow of a typical EHR with security that can be implemented in Nigeria. Figure 3 is a typical model to illustrate an architecture for the transfer of medical information

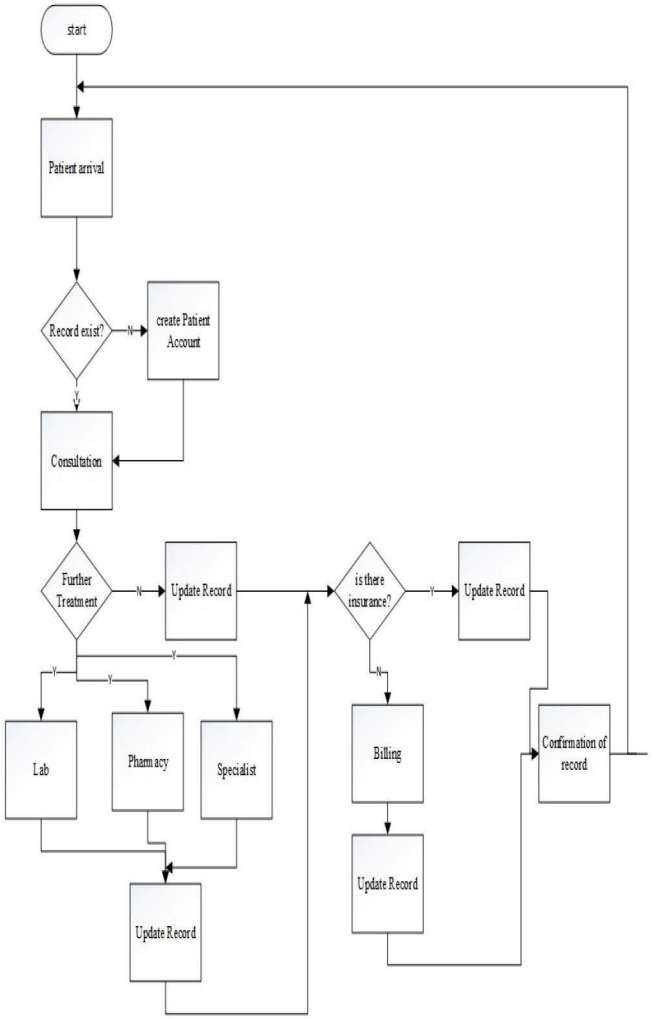

Fig 1: Flowchart of Electronic Health Record

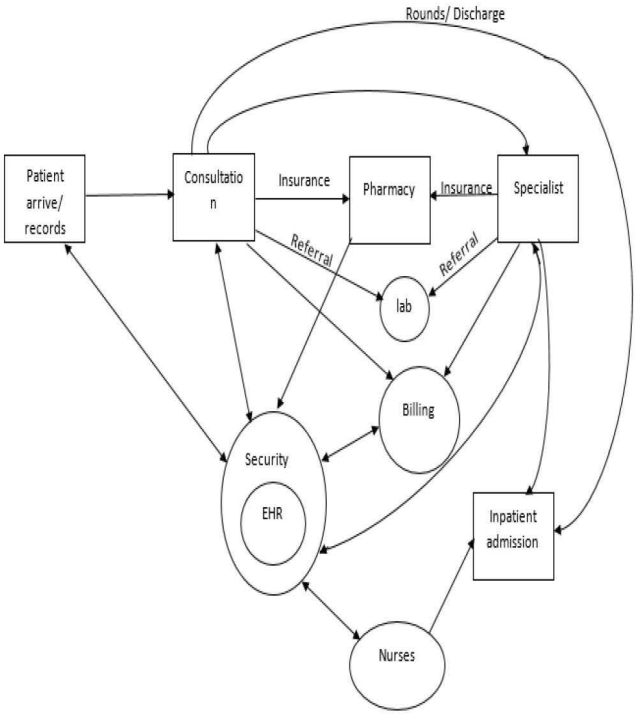

Fig 2: Data flow of Electronic health Record

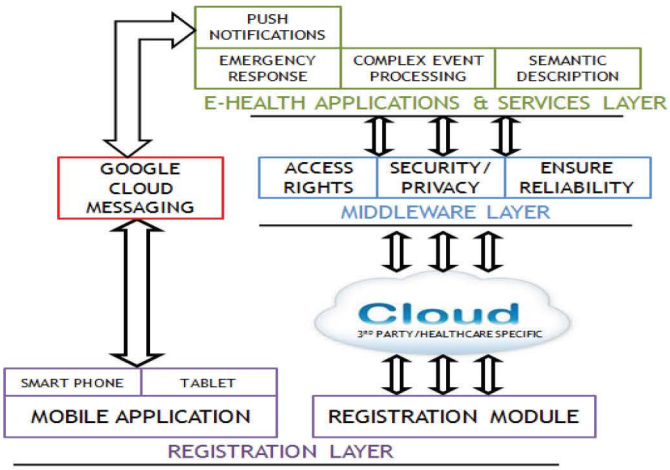

Fig 3: Illustration of the ReTiHA (Real Time Health Advice and Action) Architecture; [15]

A. Security measures in EHR

Cryptography with digital signature certificate: Public-key is commonly used to identify a cryptographic method that uses an asymmetric-key pair; a public-key and a private-key. Given a key pair, data encrypted with the public-key can only be decrypted with its private-key; conversely, data encrypted with the private-key can only be decrypted with its public-key.

Conversely, digital signature is a mechanism by which a message is authenticated i.e., proving that a message is truly coming from an acclaimed sender, much like a signature on a paper document. The message sent from the sender is encrypted with the private-key, with the public-key sent alongside the message. To successfully decrypt the message, a digital signature verification is

required to ensure that it's the sender's private-key that encrypted the message. Hashing techniques can also be used with the digital signature. The hashing algorithms are one-way encryptions, message integrity is preserved and any alteration can be easily detected. A certificate is also added to prove the identity of the sender and receiver.

Ethics: the provision of EHRs to improve medical care cannot be complete without optimal information management. The introduction of ethical obligation can be used for information management. The ethics should be in accordance with the Institute of Medicine (IOM) and Health Information Technology (HIT) rules [21].

VI. PROPOSITION FINDINGS AND RESULT

Information flow in healthcare, spans from diagnosis and treatment, medical notes, collection of data used for decision making and data exchange for outside care such as is obtainable in public health organizations [16]. Securing data is an important issue affecting various works of life, especially those in connection with information communication and technology. Government, organizations and individuals have explored various avenues to combat this prevailing situation. It has been observed that cryptography, is a technique that can maintain authentication, integrity, availability, confidentiality, identification and privacy of data.

Cryptography is the art and science of protecting information from unwanted/unauthorized persons and converting it into a form undistinguishable by potential attackers, though stored and transmitted [17]. In data cryptography, the contents which could be text, images, audio or video are scrambled during communication or storage (encrypted). This technique has received worldwide acceptance, in maximizing the security of data. A cryptographic process, involves pairs of operations like encryption and decryption or signing and verification [18]. Biometrics is a method to ensure safe authentication of a user to a portable device, most especially fingerprints which are more secure than passwords, and PIN codes. Better implementation could ensure that data is accessed only by the intended party.

The Coordination Centre, part of Carnegie Mellon University's Software Engineering Institute, had some findings while studying non-signature approaches to detection of malicious activities in the computer network traffic surveying writings, on anomaly detection and interviews from security divisions in key sectors. Evidently, organizations have improved their data security by employing engineers whose main responsibility is to query the back-end storage solutions. These engineers need to be well acquainted with the operations of the organization, including the network protocols and detectable activities, both normal and malicious. Some cyber-security operators are utilising open source software and custom storage in a bid to eradicate these security issues that change due to certain corporate events such as international conferences [19].

Success in combating cyber-security challenges, differ from one organization to another. In any instance, security in any stage, places costs on any organization [19]. In the medical sector these costs are more pronounced due to the sensitivity of data involved. This is because healthcare systems have aligned more towards the use of wireless sensor networks which started from systems with simple low profile sensors that have the capability of monitoring the location of the patient, then to complex systems like ECG (electrocardiograms), heart rate and oxygen machines [15]. Mobile devices have also evolved to smart devices, with improved memory and faster processors capable of performing better computations. These smart devices act as a means of data transfer in between the sensors and the cloud. Simple techniques such as a unique user name and password or provision for updates and alerts (in case of breaches), can go a long way in securing the data of a particular individual. Notifications could be through SMS(short message service), via a mobile phone or push notifications, through an application on a smart device which receives data from the hospital servers, and then passes it on to the patient through a cloud messaging service [15].

Security is an aspect that cannot be exaggerated. It is recommended as highlighted in a report *Trust and security challenges in cyberspace* (2000) [20] that further research be carried out in various aspects such as: Securing personal area networks comprising of personal devices which are interconnected, to store or mange large volumes of data, virtual communities and the information technology infrastructure. Hospitals and healthcare centre should provide polices, guidelines, standards and agreements pertaining to the acquisition, integrity and confidentiality of data in compliance with government regulations. These documents should be made available to all patients and staff, most especially those new to the system and facilities of the hospital or healthcare centre and records of signed agreements should be kept with the human resource management.

Review and management of general procedures such as logging in and out of systems, browsing and release of information, different access level permissions, accounting and regular audits should be a regular exercise to identify potential risks. The use of biometrics for access could offer improved security.

VII. RECOMMENDATIONS

Another method of securing data is to have two levels of information. One with basic information that can be easily accessed and the other level, more in-depth sensitive information with stricter access restrictions. Reported or identified breaches should be investigated to highlight intent, cause, effect and future avoidance, taking proper disciplinary or civil actions against offenders.

Encryption methods should be improved to provide more effective and efficient systems that do not compromise data confidentiality, integrity and security.

In view of the foregoing, suffice it to say that African governments need to strategically adopt policies that will enhance the robust implementation of EHR systems. This will go a long way in bolstering the various healthcare drives in various African countries to make healthcare accessible and affordable to all and sundry. The current manual systems that currently obtains is a major limitation

as it does not enhance effective planning and administration. It laden with file redundancies and all manner of loses and damages which these manual records are easily susceptible to. In addition, in this era where advanced society have begun to embrace telemedicine, developing countries can only dream about such. Some specializations have very scarce personnel and a robust EHR mechanism will help such professionals reach out to people from far and near, without having the traditional need of physical presence. And all these can be implemented with a robust and secure way.

VIII. CONCLUSION

Cybercrime is one of those phenomenon that may never be eradicated because it is constantly evolving with advances in technology, but potential risks can be appreciably reduced and managed. Consequently, we can infer that computerizing medical records, still poses less risk than having multiple records in different locations. The use of EHR systems ensures that data need only be collected once, "collect once, use many times". Furthermore, security is not only important in terms of authentication and testing of the systems, but also proper education of people utilizing these systems. Inappropriate access to medical information, intentional and unintentional misuse of health information should be addressed as soon as they occur. The Government should exert proper governance by adopting uniform privacy rules and regulations according to the geographical demarcations, authenticating requirements for the medical/health sector, in-depth public education and adequate awareness as it pertains to medical data, most especially the role of technology in its collection, transfer and storage. As long as the cyberspace exists, securing information will always be needed as no perfect system will ever exist. Awareness of this challenge should be fuelled constantly, to ensure individuals and the general public can identify, manage and if possible mitigate the security risks involved.

REFERENCES

[1] Cyberspace". Microsoft® Encarta® 2009 [DVD]. Redmond WA: Microsoft Corporation, 2008.

[2] Hundley R., & Anderson R. (1995). Emerging Challeges: Security and safety in cyberspace.

[3] Purewal S.J (2011): 24,000 Pentagon Files Stolen in Major Cyberattack. Retrieved from http://www.pcworld.com/article/235816/Pentagon_Files_Stolen_in_Major_Cyberattack.html on Febuary 5, 2015

[4] White J. (2011): Pentagon Seeks Cyber Security Strategy After Massive Hack of 24,000 Files. Retrieved from http://www.ibtimes.com/pentagon-seeks-cyber-security-strategy-after-massive-hack-24000-files-298825 on Febuary 5, 2015

[5] PriceWatersCoopers (PWC), (2011). Global economy crime survey.

[6] AHIMA. (2011): "Fundamentals of the Legal Health Record and Designated Record Set." Journal of AHIMA 82, no.2 (February 2011): expanded online version.

[7] Gunarto H., (n.d.). Ethical issues in cyberspace and IT society. Ritsumeika Asia Pacific University. Retrieved June, 24, 2014 from http://www.apu.ac.jp/ngunarto/it1.pdf

[8] Jones G., & Stogoski J., (2014). ALTernatives to signatures (ALTS). CERT® Coordination Centre, Software Engineering Institute.

[9] Ivanov V., Yu P., Baras J., (2010). Securing the communication of medical information using local biometric authentication and commercial wireless links. Health Informatics Journal, 16(3), 211 – 223.

[10] Rosenzeig P., (2009). National security threats in cyberspace. A workshop jointly conducted by American Bar Association Standing Committee on Law and National Security and National Strategy Forum.

[11] Crouch S., (2013). Ensuring patient privacy in cyberspace. Hospitals & health Networks (H&HN) Daily.

[12] Snyder A., & Weaver A., (2003). The e-logistics of securing distributed medical data. Department of Computer Science, University of Virginia

[13] Lagesse B., (2008). Privacy challenges for wireless medical devices. Cyberspace Sciences and Information Intelligence Research, Computational Sciences and Engineering, Oak Ridge National Laboratory.

[14] Iakovidis I. (1998) "Towards Personal Health Record: Current situation, obstacles and trends in implementation of Electronic Healthcare Records in Europe", International Journal of Medical Informatics vol. 52 no. 128, pp. 105 –117

[15] Dolui K., Mukherjee S., Datta S., Rajamani V. (2014). ReTiHA: Real Time Health Advice and Action using smart devices. St. Thomas' College of Engineering and Technology India, EURECOME Biot France, College of Engineering Trivandrum India.

[16] Rode D. (2012). Data integrity in an era of EHRs, HIEs and HIPAA: A health information management perspective. American Health Information Management Association.

[17] Tripathi R., & Agrawal S., (2014). Comparative study of symmetric and asymmetric cryptography techniques. International Journal of Advance Foundation and Research on Computer (IJAFRC), 6(1), 2348 – 4853

[18] Kanth V., Kumar K., Keerthana K., (2014). A survey on bit keys in Crytography. International Journal of Research and Applications, 1(1): 1 – 5

[19] Jones G., & Stogoski J., (2014). ALTernatives to signatures (ALTS). CERT® Coordination Centre, Software Engineering Institute.

[20] Security and privacy of electronic medical records. (n.d.), White paper. Retrieved June 26, 2014, Retrieved from http://himss.org/files/Himssorg/content/files/SecurityandPrivacyofElectronicMedical Records.pdf

[21] CGI (2004): public key encryption and digital signature: how do they work. CGI group Inc, Business solutions through information technology retrieved from:http://www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf on October 21, 2014.