International Journal of Information Security and Privacy
Volume 19 • Issue 1 • January-December 2025

‘The Way to Be Safe Is Never to Be Secure’: Security of ePHI in South African Hospitals

Kabelo Given Chuma
University of South Africa, South Africa

Mpho Ngoepe
https://orcid.org/0000-0002-6241-161X
University of South Africa, South Africa

ABSTRACT

Data security is used to protect sensitive and confidential patient health information. The healthcare sector is affected by the myriad of cybersecurity threats and attacks. Safeguarding Electronic Personal Health Information (ePHI) against cybersecurity threats and attacks is important. This study sought to explore the security of ePHI in South African hospitals with a view to proposing a framework. A qualitative study was carried out in public hospitals using semi-structured interviews with purposively selected participants of IT managers, technicians, and network controllers. The findings revealed that South African hospitals suffer from a range of cybersecurity threats, including Trojan viruses, cryptographic attacks, distributed denial of service attacks, phishing emails, password attacks, and malware attacks. The lack of security policies and poor compliance with data protection laws have been recognised as major challenges facing hospitals. The study proposes a security framework that could assist hospitals in securing ePHI by providing a set of guidelines and safeguards.

KEYWORDS

Cybersecurity, ePHI, Privacy, Confidentiality, Healthcare Facilities, Personal Information

INTRODUCTION

The aphorism by Benjamin Franklin, “The way to be safe is never to be secure,” implies that one must never feel secure in one area. This can also be applicable to patients’ health information, as such information needs to be protected against various perils. Data security has become one of the most challenging tasks that healthcare facilities around the world are facing (Puppala et al., 2016). Healthcare facilities at various levels, including hospitals, clinics, pharmacies, laboratories, and healthcare centres, are involved in the collection, extraction, and handling of patients’ health data that contains highly sensitive, personal, and confidential information in electronic and digital format for the purpose of attending to patients. This information is commonly known as electronic personal health information (ePHI), which is defined as patient health information that is computer-based and, for example, created, received, stored, maintained, processed, and/or transmitted by an electronic health care provider (Kanney, 2019). Considered the most highly sensitive and confidential type of information associated with an individual, ePHI includes patient names, surnames, dates of birth, addresses, genders, and personal contact details. It may also contain valuable information, including the medical record number, account numbers, patient demographics, date of admission and discharge, date of birth, gender, and test results.

DOI: 10.4018/IJISP.367275

There is no doubt that electronic patient information is sensitive by nature and vulnerable to a variety of intentional and unintentional threats, including unauthorised access, disclosure of information, password attacks, and dissatisfied employees. Cyber threats and attacks in the form of malware, ransomware, phishing, hacking, power and system failures, and natural disasters can disrupt healthcare systems and cause potential damage to ePHI. A growing number of security threats and attacks are being witnessed in healthcare organisations across the globe, partly because ePHI and health information systems (HISs) are widely used and adopted (Onuiri et al., 2015). Cyber threats and attacks like phishing, ransomware, malware, and distributed denial of service (DDoS) are among the top threats affecting almost all sectors across the world. Ransomware attacks are reportedly affecting 40% of government departments worldwide (Benson, 2017). The healthcare industry remains one of the prime targets for cyber threats and attacks.

Indeed, according to a recent study by the Ponemon Institute (2018), cyber threats, attacks, and breaches of ePHI in healthcare are consistently high in terms of number, size, frequency, and cost. Over the past two years, approximately 90% of healthcare organisations worldwide have experienced a growing number of data breaches, and the sector was the leading industry for cyberattacks and data breaches in 2018. A study conducted by Argaw et al.(2019) revealed that 81% of hospitals in the United States have experienced cyberattacks such as DDoS, ransomware, and phishing in 2017. Kruse et al. (2017) reported that 66% of healthcare facilities in Canada, 48% of hospitals in Australia, and 56% of hospitals in Great Britain were increasingly targeted by ransomware and phishing attacks in 2017. Additionally, the 2017 WannaCry attacks in England affected 37% of hospitals, leading to significant operational disruptions. IT News Africa (2016) reported that South African healthcare hospitals are faced with security threats and breaches such as hacking, malware, and ransomware. For instance, cybercriminals and malware targeted one of the hospitals owned by the Life Healthcare Group in South Africa during the COVID-19 pandemic.

The attack affected hospital systems and servers such as patient admission systems, business-processing systems, and e-mail servers (Bottonmley, 2020). The ePHI stored in healthcare systems has given rise to a number of privacy issues. According to Keshta and Odeh (2020), the use of electronic health records (EHR) and HISs in hospitals and healthcare facilities has raised a growing number of concerns pertaining to security and privacy issues. According to Rai and Srivastava (2014), privacy issues such as misuse and abuse of information, data leakage, and data sharing pose serious challenges to healthcare facilities. Odekunle et al. (2017) remarked that many patients in the sub-Saharan Africa region have expressed their concerns about the security and privacy of electronic health information and HISs. Despite the increasing adoption of EHR and HISs in developed countries like the United Kingdom, New Zealand, United States, Australia, and the Netherlands, several developing countries in Africa, including Nigeria, Rwanda, Kenya, Ghana, sub-Saharan Africa, and Zimbabwe, still face a plethora of challenges, such as a lack of information and communication technology (ICT) infrastructure, financial constraints, and the digital divide, to implement and adopt EHR systems (Thomas, 2016).

The digital divide and e-readiness are considered major social and cultural barriers affecting the adoption of health information technologies like EHR, e-health, and telehealth in most countries (De Lusignan et al., 2014). In contrast, other African countries like Uganda, Tanzania, and Ethiopia have successfully integrated EHR systems. These countries have experienced a growing concern about the security and privacy relating to EHRs and HISs (Vassell-Webb, 2019). Given this context, in order to overcome these security and privacy issues and concerns, it is essential for healthcare facilities to formulate security mechanisms that are intended to thwart security threats and protect ePHI. According to Liveri et al. (2021), healthcare facilities must implement a set of robust security controls, including administrative, physical, and technical security controls, to protect and secure ePHI. These three main security controls are necessary to reduce or thwart security threats to ePHI. In addition to this, Kwon and Johnson (2013) asserted that healthcare facilities must comply with regulatory requirements such as laws, regulations, legislation, and security policies designed to protect