Interpreting EHRs Privacy Paradox through Narrative Theory : A Management Perspective on Digital Health Privacy Challenges

Hanaa Farih

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Interpreting EHRs Privacy Paradox through Narrative Theory : A Management Perspective on Digital Health Privacy Challenges

Le Paradoxe de la Vie Privée dans les DSE : Approche Narrative et Management en Santé Numérique.

Auteur 1 : FARIH Hanaa.

FARIH Hanaa – PhD student,
Laboratory of Research in Finance, Audit and Governance of Organizations (LARFAGO),
National School of Business and Management – ENCG Settat, Hassan The First University, Settat, Morocco.

Déclaration de divulgation : L'auteur n'a pas connaissance de quelconque financement qui pourrait affecter l'objectivité de cette étude.

Conflit d'intérêts : L'auteur ne signale aucun conflit d'intérêts.

Pour citer cet article : FARIH .H (2024) « Interpreting EHRs Privacy Paradox through Narrative Theory : A Management Perspective on Digital Health Privacy Challenges », African Scientific Journal « Volume 03, Numéro 22 » pp: 0376 – 0404.

Date de soumission : Janvier 2024

Date de publication : Février 2024

DOI : 10.5281/zenodo.10656947

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Abstract

The present paper delves into the privacy paradox in Electronic Health Records (EHRs) from the perspective of digital health management, employing narrative theory and a multifaceted analysis of factors influencing individuals' perceptions of privacy risks and benefits associated with EHRs. It scrutinizes how cognitive biases, a lack of awareness or understanding of privacy risks, the prioritization of convenience over privacy concerns, trust in healthcare systems or technology providers, and the perceived benefits outweighing perceived risks collectively shape user behavior and decision-making regarding EHR privacy. The methodological approach is rooted in the application of Narrative Theory, providing a theoretical lens through which the dynamics of the Privacy Paradox are explored, rather than empirical data collection. The results of the conceptual literature review underscore the strategic importance of addressing cognitive biases, enhancing privacy awareness, prioritizing privacy in the user experience, cultivating trust, and communicating balanced narratives about the benefits and risks. This paper emphasizes the integration of narrative-driven strategies into digital health management practices, particularly in privacy communication, patient education, and EHR system design, as effective approaches to navigate the privacy paradox and foster informed decision-making among EHR users. The main conclusion drawn is that Narrative Theory offers a profound framework for understanding and addressing the Privacy Paradox in EHRs, suggesting that a narrative-driven approach in digital health management can significantly contribute to resolving the paradox. The application of Narrative Theory within the realm of digital health management offers a novel perspective, enriching academic discourse and providing researchers and practitioners with a fresh lens to understand and address the Privacy Paradox in EHRs.

Keywords : Privacy Paradox, Digital Health Management, Patient Behavior, Electronic Health Records, Narrative Theory.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Résumé

L'article se penche sur le paradoxe de la vie privée dans les Dossiers de Santé Électroniques (DSE), adoptant la perspective du management digital de la santé. Il utilise la théorie narrative et analyse divers facteurs influençant la perception des risques et avantages de confidentialité liés aux DSE. Il examine comment les préjugés cognitifs, le manque de sensibilisation ou de compréhension des risques, la priorisation de la commodité, la confiance dans les systèmes de santé ou les fournisseurs de technologie, et les avantages perçus surpassant les risques perçus, façonnent le comportement des utilisateurs et la prise de décision en matière de confidentialité des DSE. L'approche méthodologique repose sur l'application de la Théorie Narrative, examinant les dynamiques du paradoxe de la vie privée à travers un prisme théorique plutôt que par la collecte de données empiriques. Les résultats soulignent l'importance de s'attaquer aux biais cognitifs, d'améliorer la sensibilisation à la protection de la vie privée, de prioriser cette dernière dans l'expérience utilisateur, de cultiver la confiance et de communiquer des récits équilibrés sur les avantages et les risques. La conclusion principale révèle que la Théorie Narrative offre un cadre significatif pour comprendre et adresser le paradoxe de la vie privée dans les DSE, suggérant qu'une approche centrée sur le récit peut contribuer de manière significative à sa résolution. L'application de cette théorie dans le management digital de la santé enrichit le débat académique, offrant aux chercheurs et praticiens un nouveau prisme pour aborder le paradoxe.

Mots-clé : Paradoxe de la vie privée, Management Digital de la Santé, comportement des patients, Dossiers de Santé Electroniques, Théorie Narrative.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

1. INTRODUCTION

EHRs have become increasingly prevalent in healthcare settings due to their potential benefits in improving patient care, enhancing coordination among healthcare providers, and facilitating research and population health management. As one of the most obvious manifestations of Digital Health Mnagement, these electronic records have transformed the way in which patient data is collected and managed, offering a comprehensive digital platform for healthcare professionals (McKeeby & Coffey, 2018). However, the widespread use of EHRs has also brought to light a privacy paradox - the intricate balance between personalization, privacy protection, and security controls. While EHRs have the potential to revolutionize healthcare, there are significant concerns regarding patient-controlled access and data confidentiality (Shah & Khan, 2020).

The exponential growth of EHR data has presented numerous challenges, as it is large, heterogeneous, and often incomplete (Yüksel et al., 2017). Furthermore, the noisy nature of EHR data has made it difficult to utilize for research purposes (Coorevits et al., 2013). Overcoming these challenges has become possible through the application of computer science artificial intelligence techniques, particularly natural language processing and machine learning (Lin et al., 2021). Despite this progress, the journey towards a "complete EHR" is far from over. As we embrace the advancements in managing EHR data through artificial intelligence, we must also confront the growing concerns over patient privacy, a crucial aspect intertwined with the evolution of these digital health systems. Privacy concerns in EHRs are recognized as a fundamental requirement and one of the formidable challenges affecting the trust and acceptability of these systems (Rezaeibagha et al., 2015). While EHRs offer numerous benefits, such as improved patient care and data accessibility, they also raise concerns about patient privacy. These concerns stem from the potential unauthorized access to sensitive health information, improper use of data, and the lack of control that individuals have over their own health information.

In our attempt to delve into the complexities surrounding privacy in Electronic Health Records, it becomes evident that the theoretical concerns about data confidentiality and security often contrast sharply with the actual behaviors of both healthcare providers and patients. This dichotomy brings us to a critical junction in our discussion : the **Privacy Paradox**. It refers to the cognitive dissonance between individuals' concerns about privacy and their actual behaviors that may compromise their own privacy (Keshta & Odeh, 2021). Therefore, navigating the Privacy Paradox in Electronic Health Records requires a comprehensive understanding of the

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

regulations, technologies, and factors impacting individual's privacy concerns (Meingast et al., 2006).

The gap between patients' expressed privacy concerns and their actual data-sharing behaviors must be understood as electronic health records (EHRs) become more and more essential to modern healthcare. Which raises the following pivotal question : **what factors behind the privacy paradox in EHRs ?**

Hereafter, the subject of this study is the Privacy Paradox in EHRs, which critically analyzes the disparity between people's stated worries about privacy and their real actions that could jeopardize it in the context of managing digital health. Through the use of narrative theory, the goal of this study is to investigate the underlying factors—cognitive biases, awareness levels, convenience prioritization, trust, and perceived benefits against risks—that impact this paradoxical behavior. The methodological basis of this study is narrative theory with respect to the intricate notion of the Privacy Paradox in EHRs. This theoretical framework was specifically chosen because it effectively explains the distinctions between declared privacy concerns and potential counteracting activities.

Narrative theory allows a comprehensive examination of the human psyche by demonstrating how cognitive biases, awareness levels, convenience priority, trust, and perceived benefits vs risks combine to form user behavior in digital health contexts. This theory provides a comprehensive framework that not only clarifies the intricate connection between identity and privacy, but also transcends traditional analytical boundaries to enable a more nuanced comprehension of privacy concerns. The constructivist paradigm, which underpins this research's epistemological approach, maintains that personal narratives that are formed and shared by communities and individuals dynamically influence and reshape people's views of privacy.

By giving weight to the individual interpretations and meanings that people ascribe to their experiences, this approach enables the articulation of a more comprehensive narrative that strikes a balance between the theoretical underpinnings of the Privacy Paradox and the day-to-day realities of EHR management.

This work is organized as follows : first, the theoretical foundation of the Privacy Paradox is outlined ; next, an in-depth examination of Narrative Theory, our methodological lens for analysis, is covered. The theory's applicability to the EHR dilemma will be examined in more detail in the following sections, along with its implications for digital health management. Our findings will be summarized in the conclusion, along with suggestions for further study and real-world applications for handling privacy issues in the context of digital health.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

2. THEORETICAL FRAMEWORK : PRIVACY PARADOX

2.1. Conceptual definition :

The Privacy Paradox theory refers to the phenomenon where individuals simultaneously express concerns about their privacy while engaging in behaviors that seem to compromise it. Ektor et al. (2023) define the privacy paradox as the inconsistency between privacy concerns and actual behavior that leads to the dominance of privacy-careless platforms. This theory suggests that individuals may value privacy in principle, but when faced with the benefits and convenience offered by new technologies, they are often willing to trade some of their privacy for these perceived benefits.

Researchers in psychology also have examined this phenomenon and reported that part of the reason for this behavior is believed to be an "evolutionary mismatch." These preconceived notions regarding privacy are out of date with the online world of today, having originated in the predigital period. Because of this mismatch, there is a gap between the concerns and the actions of individuals, making it difficult for them to identify or effectively address contemporary dangers to online privacy (Shariff et al., 2021).

Another way to conceptualize the privacy paradox is as a discrepancy between individuals' expressed concerns about their privacy and their willingness to share personal information in practice (Barth & Jong, 2017). Despite acknowledging the importance of privacy, individuals may still engage in behaviors that involve disclosing personal data, often due to the perceived benefits or convenience of the services or technologies they are using. This paradox highlights the complex interplay between privacy concerns and the trade-offs individuals make in their interactions with digital platforms and technologies.

This trade-off between privacy concerns and perceived benefits can be attributed to several factors. These factors include a lack of awareness or understanding about the potential risks to privacy, an emphasis on immediate gratification and convenience, overestimation of the adequacy of privacy controls, trust in institutions or technologies, social norms, and the perception of personal control over privacy (Kokolakis, 2017).

Tobias et al. (2021) in their longitudinal analysis of the privacy paradox stated that people's concerns about online privacy are not reflected in their actual behavior of sharing personal information online. In their study, They found that individuals who expressed high levels of privacy concerns were still engaging in behaviors that involved sharing personal information

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

online. This inconsistency between privacy concerns and behavior is at the core of the privacy paradox.

However, it is important to note that the privacy paradox may not be a universal phenomenon (Dienlin & Trepte, 2014), as cultural and contextual factors can also influence individuals' attitudes and behaviors towards privacy. Thus, it is crucial to acknowledge the nuanced nature of the privacy paradox and consider the various factors that contribute to this phenomenon.

Furthermore, the privacy paradox is not limited to the online context (Tobias et al, 2021), even if this paradox is often discussed in the context of internet usage, social media platforms, and digital technologies. Similar patterns can also be observed in other, non-digital contexts as well. For example, someone might voice concerns about personal privacy but still share sensitive information in face-to-face conversations, or sign up for loyalty programs without reading the privacy policies, or neglect to shred personal documents before disposal. Accordingly, it is important to understand that the privacy paradox is a complex issue influenced by various individual and contextual factors. For example, attitude certainty plays a role in the correspondence between privacy attitudes and data disclosure. Lower attitude certainty is associated with a lower correspondence between attitudes toward data disclosure and online behavior.

Additionally, in the context of online social networking, the need for self-identity is a key factor affecting people's privacy behavior (Philip, F. W., 2019). The urge for self-expression and identity formation supersedes the traditional concept of privacy in the world of online social networks. The so-called "privacy paradox" is not a paradox per se in this context, as privacy concerns reflect the ideology of an autonomous self, while self-identity explains voluntary self-disclosure (Marco, V., 2019).

Therefore, the privacy paradox can be observed in various contexts, including online social networking and the disclosure of health data information in online forums and communities (Chrysanthi et al., 2017), and its resolution requires a multifaceted approach that includes education, policy interventions, and technological advancements., including cultural norms, societal attitudes towards privacy, and the specific context in which individuals are making decisions about their personal information.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

2.2. Theorectical underpinnings of Privacy Paradox :

The theoretical underpinnings of the privacy paradox are based on several concepts.

2.2.1. Social norm

One important explanation is the concept of social norm, which suggests that individuals' decisions to accept or reject a specific platform are influenced by their social environment. Influences from social norms can significantly impact individual decision-making when it comes to privacy and personal data disclosure. The expectations, beliefs, and behaviors that are prevalent in a person's social circle and broader society play a substantial role in shaping their attitudes towards privacy. Individuals may conform to these social norms and disclose personal information online even if they have concerns about privacy, leading to the privacy paradox (Dienlin et al., 2019).

Moreover, social structures and norms can constrain individuals' autonomy and influence their privacy-related decisions. People may feel compelled to disclose personal information due to social pressures, fear of social exclusion, or the desire to conform to societal expectations. The impact of social norms on the privacy paradox extends beyond individual decision-making and can encompass broader cultural attitudes towards privacy. Cultural norms and values related to privacy vary across different societies and can significantly influence how individuals perceive and prioritize their privacy concerns. For instance, in some cultures, the collective welfare or societal harmony may take precedence over individual privacy, leading to differing attitudes and behaviors towards privacy-related decisions.

2.2.2. Risk-benefit evaluation theory / Privacy calculus

The theory of risk-benefit evaluation posits that individuals make decisions about sharing personal information based on their perceived balance between the potential benefits and risks involved. They weigh the potential advantages gained from sharing their personal information, such as personalized services, targeted advertisements, or social connectivity, against the potential negative consequences of privacy breaches, identity theft, or misuse of data (Shih & Liu, 2023). This evaluation of risks and benefits forms the basis of the decision-making process, wherein individuals weigh the potential advantages of disclosure against the potential threats to their privacy.

Furthermore, the risk-benefit evaluation theory is often intertwined with the concept of privacy calculus, which emphasizes the continual reassessment of privacy choices based on evolving perceptions of risks and benefits. Privacy calculus posits that individuals engage in an ongoing

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

evaluation of the trade-offs between privacy concerns and the potential benefits derived from sharing personal information (Li, 2012). This dynamic process of reassessment reflects individuals' responses to changes in their perceptions of risks and benefits. By continually evaluating and reevaluating the risks and benefits, individuals can adapt their privacy-related decisions to align with their evolving needs and circumstances.

In the same vein, privacy calculus encompasses the notion of privacy management, wherein individuals actively engage in strategies to regulate the disclosure of their personal information. This involves implementing privacy-enhancing measures, adjusting privacy settings, and making informed decisions about the extent to which they are willing to share their data. Privacy management reflects the agency and control individuals exercise in navigating the intricate landscape of privacy concerns and benefits, further illuminating the complexities encapsulated within the privacy paradox.

2.2.3. Dual process theory

Another theoretical basis is the dual process theory, which considers conscious and unconscious modes of decision-making processes. This theory, conceptualized by Daniel Kahneman and Amos Tversky (Tversky & Kahneman, 1982), emphasizes the coexistence of these two parallel systems of thought – System 1 and System 2. System 1 represents the intuitive, automatic mode of thinking, whereas System 2 encapsulates the deliberate, analytical thought processes. This model of dual processing recognizes that individuals' privacy-related decisions are influenced by a combination of intuitive, emotionally driven responses and reasoned, conscious evaluations.

On one hand, unconscious processes such as social influence, habitual behavior, and emotional responses can shape individuals' privacy decisions. On the other hand, individuals may consciously weigh the risks and benefits of sharing personal information, considering factors such as trustworthiness of the platform, data sensitivity, and potential consequences. (James et al., 2015).

2.2.4. Elaboration likelihood model (ELM)

The Elaboration Likelihood Model (ELM) is also used to understand the cognitive processes underlying data disclosure decisions. It is a widely used framework for understanding the cognitive processes underlying persuasion and decision-making. Developed by Richard E. Petty and John T. Cacioppo (Petty & Cacioppo, 1986), the ELM posits that individuals' attitudes and decisions are influenced by two distinct routes : the central route and the peripheral route.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

- → The central route involves a deep and thoughtful processing of relevant information. When individuals are motivated and able to engage in careful evaluation, they consider the merits of the arguments or information presented to them. This route requires cognitive effort and critical thinking as individuals weigh the logic, evidence, and quality of the messages before forming attitudes or making decisions.
- → The peripheral route, on the other hand, relies on simpler cues and heuristics to make quick judgments and decisions. When individuals lack motivation or cognitive resources to deeply process information, they may be swayed by peripheral cues such as the attractiveness of the source, the emotional appeal of the message, or the presence of consensus or authority figures. In this route, individuals may form attitudes or make decisions based on superficial aspects of the communication rather than the substantive content.

In the context of privacy-related decisions, the ELM offers valuable insights into how individuals evaluate and respond to information related to data disclosure. When individuals are presented with privacy-related messages or requests, their level of motivation and ability to process the information can influence whether they engage in central or peripheral processing. Factors such as the perceived relevance of the information, personal relevance of the privacy decision, and cognitive resources available to the individual can determine the route of processing.

2.3. Application to EHRs :

In the context of Electronic Health Records, navigating the Privacy Paradox becomes especially challenging due to the sensitive nature of healthcare data and the importance placed on protecting patient privacy (Perera et al., 2011). The manifestation of the Privacy Paradox in Electronic Health Records underscores the complexities of patient and healthcare provider behavior in the digital healthcare landscape. Despite the recognized importance of safeguarding patient privacy and sensitive health information, the advent of EHRs has introduced a unique set of challenges that contribute to the Privacy Paradox.

2.3.1. Patients' Dilemma :

For patients, the Privacy Paradox materializes in the form of conflicting desires and concerns regarding the disclosure of personal health information through EHRs. On one hand, patients recognize the potential benefits of EHRs in terms of streamlined care coordination, improved

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

medical decision-making, and enhanced accessibility to their health records. However, these perceived advantages are juxtaposed with apprehensions about the security and confidentiality of their sensitive health data within the digital ecosystem. As a result, patients may exhibit cautious behavior, such as selectively disclosing certain health information or expressing reluctance in actively engaging with EHR platforms (Shen et al., 2019). This reluctance stems from the overarching fear of privacy breaches, unauthorized access, or misuse of their health records, reflecting the inherent tension between the benefits of digital health information sharing and privacy preservation.

2.3.2. Healthcare Providers' Approach :

Conversely, healthcare providers are confronted with their own set of challenges arising from the Privacy Paradox in EHRs. The allure of EHRs lies in the promise of efficient information retrieval, seamless data exchange, and comprehensive patient care documentation. This perceived efficacy often drives healthcare providers to prioritize the utilization of EHR systems, occasionally overshadowing concerns related to patient privacy and data security (Entzeridou et al., 2018). While the convenience and practicality of EHRs are undeniable, the inherent trade-offs between accessibility and privacy protection present healthcare providers with a formidable quandary. In some instances, this may lead to inadvertent oversight of privacy risks or a reliance on the assumption that system safeguards are sufficient, inadvertently contributing to the Privacy Paradox within the healthcare domain.

2.3.3. Implications on Patient-Provider Dynamics :

The ramifications of the Privacy Paradox in EHRs are not only limited to individual responses but also extend to the intricacies of patient-provider interactions and the dynamics of healthcare delivery (Caine & Tierney, 2014). This different behavior can be attributed to several factors. One factor is that patients may have a higher level of personal investment and emotional attachment to their health information, leading them to experience heightened privacy concerns. Another factor is the perceived benefits and value of EHRs for healthcare providers, who may view access to comprehensive patient information as necessary for making accurate diagnoses and providing appropriate treatment.

The convergence of divergent privacy perceptions between patients and healthcare providers can potentially lead to a discordance in the exchange of health information, impede the establishment of a fully transparent patient-provider relationship, and undermine the holistic integration of EHRs into healthcare practices.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

3. Literature Review : Challenges of Maintaining Privacy in EHRs

Historically, privacy concerns in healthcare data management have been evident long before the widespread adoption of EHRs. Before the advent of EHRs, patient information was primarily stored in paper-based records and kept within the confines of healthcare facilities. Unauthorized access and breaches of patient information were still a concern, but the scale and potential impact of such incidents were relatively limited. With the transition to electronic health records, privacy concerns have intensified due to the increased accessibility of patient information and the potential for data breaches on a larger scale (Meingast et al., 2006).

The existing literature provides valuable insights into the specific challenges of maintaining privacy in EHRs. Several scholarly works have focused on devising frameworks and technologies to address the complexities associated with privacy preservation in digital healthcare environments.

One challenge is the risk of patient data theft and misuse (Graves, 2013), and this poses a significant threat to the confidentiality and integrity of electronic health records. Unauthorized access to EHRs can lead to the misuse of sensitive patient data, including identity theft, insurance fraud, and unauthorized medical procedures. Additionally, the potential for data breaches in EHRs can have far-reaching consequences, such as compromising patient trust, violating regulatory requirements, and exposing healthcare organizations to legal and financial repercussions.

Furthermore, the inherent complexity of EHR systems, coupled with the interconnected nature of healthcare information exchange, amplifies the challenges related to access control and privacy management (Sharathkumar et al., 2017). Effective access control mechanisms are crucial for safeguarding EHRs against unauthorized viewing, modification, or dissemination of patient data. However, ensuring stringent access control measures while maintaining seamless data accessibility for authorized healthcare professionals remains a delicate balance.

Another challenge is the need to provide proper therapy while ensuring access to relevant information (Beard et al., 2012). This challenge requires striking a balance between privacy and the flow of information for healthcare functions. Balancing the imperative of safeguarding patient privacy with the essential dissemination of pertinent healthcare information is a complex task that demands careful navigation (Miron-Scahtz et al., 2011).

Furthermore, the interoperability of health information systems poses a challenge to privacy in EHRs (Ghazvini & Shukur, 2013). Accordinglly, enforced privacy and privacy in the presence of others are highlighted as major challenges in e-health in general and EHRs in partiular.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Enforced privacy pertains to the difficulty of maintaining privacy while ensuring interoperability among different subsystems, and privacy in the presence of others addresses the need to protect sensitive health information in shared or group settings.

Another challenge would be the integration of various data types in EHRs, such as clinical data (information collected from patient healthcare interactions, including medical history, diagnoses, treatments, and lab results), genetic data (data related to an individual's genes and DNA, providing insights into genetic traits and predispositions to certain health conditions), and lifestyle information (details about a person's daily habits and choices, such as diet, exercise, and substance use, relevant to their overall health and wellness). This diversity of patient's information raises complex privacy concerns due to the sensitive and personal nature of these data. The combination of these different data types in EHRs creates a comprehensive profile of an individual's health, which can provide valuable insights for personalized treatment and care. However, the integration of these diverse data types also increases the risk of privacy breaches and unauthorized access (Jensen et al., 2012). This is especially true for genetic data, which can reveal a wealth of personal information and has the potential for misuse if not protected properly.

We can also cite the challenges in securing EHRs stored in the cloud, focusing on access control, data privacy, and scalability issues (Gautam et al. 2019). Establishing robust access control mechanisms is critical to preventing unauthorized viewing, modification, or dissemination of sensitive patient data. The distributed nature of cloud storage introduces complexities in managing access permissions across diverse healthcare entities and providers. Furthermore, the authentication of legitimate users and the protection against insider threats are critical considerations in the design and implementation of secure cloud-based EHR systems. The preservation of data privacy and confidentiality is another significant challenge in the context of EHRs stored in the cloud. Scalability issues also pose a notable challenge in securing EHRs stored in the cloud. As the volume of electronic health records continues to grow, the scalability of security measures and infrastructure becomes crucial to effectively manage and protect the expanding dataset.

On the same vein, we can not discuss the challenges of maintaining privacy in EHRs without mentioning the impact of legal and regulatory frameworks on EHR privacy. Healthcare providers operating in multiple jurisdictions face significant challenges in complying with different legal and regulatory frameworks such as the General Data Protection Regulation (GDPR) in the EU and the Health Insurance Portability and Accountability Act (HIPAA) in the US.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

The GDPR, implemented by the European Union, imposes strict requirements on the protection and processing of personal data, including health information. Healthcare providers operating within the EU or handling the personal data of EU citizens must adhere to the GDPR's stringent standards. This includes obtaining explicit consent for data processing, ensuring the encryption and pseudonymization of sensitive data, and promptly reporting data breaches to the appropriate regulatory authorities. The GDPR also introduces the concept of the "right to be forgotten," allowing individuals to request the erasure of their personal data under certain circumstances.

On the other hand, healthcare providers in the US must navigate the complexities of HIPAA, which sets forth standards for the protection of individually identifiable health information. HIPAA requires healthcare organizations to implement comprehensive security measures, such as access controls, encryption, and audit trails, to safeguard electronic health records. Additionally, HIPAA's Privacy Rule governs the permissible uses and disclosures of protected health information, imposing strict limitations on when patient information can be shared without authorization.

The challenge for healthcare providers operating in multiple jurisdictions lies in reconciling the divergent requirements of these regulatory frameworks. While GDPR and HIPAA share common goals of protecting patient privacy and data security, there are nuanced differences in their scope, requirements, and enforcement mechanisms. Healthcare organizations must invest significant effort and resources to develop compliance strategies that accommodate the contrasting provisions of these regulations. This includes conducting comprehensive assessments to align their privacy and security practices with the specific requirements of each jurisdiction, implementing technical and organizational measures tailored to each framework's specifications, and developing comprehensive training programs to ensure staff awareness and adherence to the distinct regulatory requirements (Seddon & Currie, 2013).

4. Analysis of the Privacy Paradox in EHRs

As clearly established earlier, the Privacy Paradox theory suggests that individuals may have contradictory beliefs and behaviors regarding privacy. For example, individuals may express concerns about the privacy and security of their health information, but still willingly share personal data on social media or through online platforms like electronic health records. This can be explained by several factors that we will unpack through the lens of the narrative theory.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

4.1. Leveraging the Narrative Theory

Narrative theory refers to the study and analysis of storytelling and the ways in which narratives shape our understanding of the world. It explores how stories are created, interpreted, and used to construct meaning and identity in various contexts (Langer & Ribarich, 2008). Narrative theory has been applied in fields such as health communication, translation and interpreting studies, children's literature, and natural language processing. In health communication, narrative theory offers insights into the human experience of health, illness, and wellness, and how narratives can be used for activism (Vincenzo, S., 2022).

The use of narrative theory in the context of electronic health records can provide valuable insights into how individuals construct their understanding of privacy and security in healthcare, and how their attitudes and behaviors towards privacy may impact healthcare practices. Additionally, by applying narrative theory to the analysis of privacy in EHRs, researchers can uncover the underlying narratives that influence individuals' decision-making processes regarding the disclosure and sharing of their health information. This understanding can inform the development of more effective communication strategies and interventions that address individuals' concerns and enhance their privacy protection in electronic health records. By understanding these narratives, healthcare professionals and policymakers can design interventions and strategies that align with individuals' beliefs and values, ultimately promoting better privacy practices in EHRs. These discrepancies in individuals' beliefs and behaviors regarding privacy have significant implications for healthcare delivery and policy. Firstly, these discrepancies can impact healthcare delivery by creating challenges in maintaining patient privacy and confidentiality. Healthcare providers may struggle to ensure that sensitive patient information is appropriately protected and accessed only by authorized individuals. Additionally, the privacy paradox may lead to individuals withholding important health information or being hesitant to seek healthcare services if they fear their personal information may be compromised. Moreover, these discrepancies can affect healthcare policy by influencing the development and implementation of regulations and guidelines related to privacy and security in EHRs. Regulations and guidelines must take into account the diverse narratives and beliefs surrounding privacy in order to strike a balance between protecting patient information and enabling efficient healthcare delivery.

Thus, the application of Narrative Theory as an « umbrella theory » offers a comprehensive lens to understand the Privacy Paradox in EHRs. It allows to encapsulate various influencing factors within a singular narrative framework. This approach allows for a holistic understanding of how individuals construct and navigate their privacy-related narratives in the context of

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

digital healthcare. It acknowledges the complexity of human behavior and the influence of narrative on how we behave, especially when it comes to using technology. Besides, this framework extends beyond conventional analyses that concentrate exclusively on statistical patterns or isolated psychological elements, providing a broader view of how people interpret and justify how they deal with privacy.

4.2. Factors pooled by the Narrative Theory

4.2.1. Cognitive Biases

Initially, cognitive biases play a significant role in the privacy paradox observed in EHRs. These biases are systematic patterns of deviation from rationality in judgment and decision-making, often stemming from mental shortcuts and emotional influences (Waldman, 2020). In the context of privacy in EHRs, several cognitive biases can contribute to the discrepancies between individuals' attitudes and behaviors towards privacy.

One prominent cognitive bias is the illusion of control, where individuals overestimate their ability to manage and control the dissemination of their personal information (Langer, 1975). In the case of EHRs, patients may believe they have more control over who accesses their health information than they actually do, leading them to disclose sensitive data without fully considering the implications. This bias can result in individuals sharing health information in EHRs under the false belief that they can easily retract or limit its accessibility, contributing to the privacy paradox.

Moreover, the availability heuristic bias can influence individuals' perceptions of privacy risks in EHRs (Sundar et al., 2020). This bias leads people to assess the probability of an event based on how easily similar instances come to mind. In the context of EHRs, if individuals have not personally experienced a privacy breach or data misuse, they may underestimate the likelihood of such events, leading them to be less cautious about sharing their health information.

Additionally, the optimism bias can lead individuals to believe that they are less susceptible to privacy breaches and data misuse than others, leading them to engage in behaviors that compromise their privacy in EHRs.

Narrative Theory can explain how individuals construct stories influenced by cognitive biases (such as optimism bias or confirmation bias) to rationalize their behavior concerning privacy in EHRs. Narrative Theory can provide insights into how individuals construct stories influenced by cognitive biases to rationalize their behavior concerning privacy in electronic health records. Individuals may create narratives that align with their cognitive biases, such as the optimism

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

bias or confirmation bias, to justify their decisions and actions regarding the disclosure of personal health information in EHRs.

For example, individuals exhibiting optimism bias may create narratives that emphasize their belief in their ability to control who accesses their health information or their perceived invulnerability to privacy breaches. This narrative may manifest as a sense of overconfidence in their capacity to safeguard their privacy in EHRs, leading them to disclose sensitive information without fully considering the potential risks. Similarly, individuals influenced by confirmation bias may construct narratives that reinforce their existing beliefs about the safety and security of EHRs, seeking out information or experiences that validate their positive perceptions and downplay potential privacy concerns.

These constructed narratives, influenced by cognitive biases, not only shape individuals' attitudes and behaviors towards privacy in EHRs but also impact their decision-making processes and interactions with healthcare providers and technologies. By acknowledging the role of narrative theory in the context of cognitive biases, healthcare professionals and policymakers can develop targeted interventions and communication strategies to address these constructed narratives and mitigate the privacy paradox observed in EHRs.

4.2.2. Lack of Awareness or Understanding of Privacy Risks :

Many individuals may not fully comprehend the potential privacy risks associated with electronic health records, leading to a lack of awareness or understanding of these risks. This lack of awareness or understanding can contribute to individuals underestimating the importance of privacy and feeling less motivated to protect their personal health information in EHRs (Campos-Castillo & Anthony, 2014). As a result, they may engage in behaviors such as sharing sensitive information without considering potential consequences or neglecting to properly secure their EHR accounts and passwords.

Through narrative construction, individuals may downplay or ignore privacy risks. Their personal narratives might not incorporate a full understanding of these risks, reflecting a lack of awareness. This lack of awareness can be attributed to various factors, including limited education and information about privacy issues in EHRs, a lack of transparency in data handling practices by healthcare organizations, and the complexity of privacy policies and technical jargon used in EHR systems. Additionally, individuals may also lack the technical knowledge or digital literacy skills necessary to understand and navigate the privacy settings and security features provided by EHR systems.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Thus, in narrative theory, the construction of stories influenced by this lack of awareness or understanding of privacy risks can manifest as a limited acknowledgment of the potential consequences of sharing sensitive information in EHRs, contributing to an underestimation of privacy risks. This reflection of a lack of awareness highlights the importance of addressing knowledge gaps and enhancing individuals' understanding of privacy risks in EHRs.

4.2.3. Convenience Prioritization Over Privacy Concerns :

The prioritization of convenience over privacy concerns in electronic health records is a significant factor contributing to the privacy paradox observed in healthcare settings. Individuals often prioritize the ease of access and use of EHRs, valuing the streamlined communication with healthcare providers and the convenience of accessing their personal health information (Shen et al., 2019). However, in doing so, they may overlook or underestimate the potential privacy risks associated with sharing sensitive health information in EHRs.

The convenience prioritization over privacy concerns can be attributed to several factors. Firstly, the seamless access to one's health records and the ability to share information across healthcare providers contribute to improved care coordination and timely decision-making. Individuals may prioritize this convenience as it enhances the efficiency and effectiveness of their healthcare management.

Moreover, the increasing integration of digital health technologies and telemedicine platforms further emphasizes the convenience of EHRs in facilitating remote consultations and virtual care delivery. This trend has been particularly accelerated during the COVID-19 pandemic, as individuals have sought convenient and accessible ways to engage with healthcare services while minimizing in-person interactions.

Additionally, the user-friendly interfaces and accessibility features of EHR systems make it easier for individuals to navigate through their health information and actively engage in their own care. The empowerment and autonomy gained from accessing personal health data can lead individuals to prioritize the convenience of EHRs over potential privacy risks.

In narrative construction, individuals may create stories that emphasize the positive impact of convenient access to EHRs on their healthcare management, downplaying the potential privacy implications. These narratives may underscore the value of timely communication with healthcare providers and the seamless retrieval of health information, reinforcing the prioritization of convenience over privacy concerns.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

4.2.4. Trust in the Healthcare System or Technology Providers :

Trust is a significant factor that influences individuals' acceptance and usage of technology in availing healthcare services, including EHRs. Studies have shown that perceived usefulness, perceived ease of use, trust, and privacy concerns act as direct predictors of patients' behavior in accepting technology in healthcare settings. The level of trust individuals have in the healthcare system or technology providers affects their willingness to adopt and use EHRs (Dhagarra et al., 2020).

Individuals' trust in the healthcare system or technology providers can significantly impact their willingness to disclose personal health information in EHRs. When individuals lack trust in the security measures and data handling practices of healthcare organizations or technology providers, they may exhibit reluctance or skepticism in sharing sensitive health information. This mistrust can stem from concerns about data breaches, unauthorized access to their health records, or the misuse of their personal information.

Furthermore, trust in EHR systems is closely associated with the perceived privacy and security of personal health information. Individuals who have confidence in the privacy protection mechanisms implemented within EHRs are more likely to feel comfortable disclosing their health data and engaging with digital healthcare platforms. On the other hand, a lack of trust in the privacy and security features of EHRs can lead to heightened privacy concerns and resistance in utilizing electronic health records for information sharing and healthcare management.

Trust in healthcare providers and technology systems can be framed as a narrative that shapes individuals' perceptions and actions regarding the privacy of their electronic health records. The stories individuals construct about their experiences with healthcare providers and technology systems influence their attitudes and behaviors towards the security and reliability of EHRs.

In the narrative construction of trust, individuals may emphasize their positive interactions with healthcare providers and the seamless experience with technology systems, highlighting the reliability and security they perceive in the management of their health information. These narratives reinforce the trust they have in the healthcare system and the technology providers, shaping their willingness to engage with EHRs and share personal health data.

Conversely, narratives influenced by a lack of trust may reflect individuals' concerns about the security and reliability of EHRs. Their stories may underscore the uncertainties and fears associated with potential data breaches or unauthorized access to their health records, leading to hesitance in utilizing electronic health records for information sharing and healthcare management.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

4.2.5. Perceived Benefits Outweighing Perceived Risks :

The privacy paradox in electronic health records often arises from the perception that the benefits of utilizing EHRs outweigh the perceived risks to privacy. This phenomenon occurs when individuals weigh the potential advantages of convenient access to healthcare information and improved care coordination against the possible privacy implications of sharing sensitive health data in digital platforms (Entzeridou et al., 2018).

Perceived benefits, such as enhanced communication with healthcare providers, streamlined access to personal health information, and empowered engagement in healthcare management, can lead individuals to prioritize the convenience and efficiency offered by EHRs. In doing so, they may downplay or underestimate the potential risks to their privacy and confidentiality associated with sharing personal health data in electronic formats.

In constructing narratives about the perceived benefits of EHRs outweighing the perceived risks, individuals may emphasize the transformative impact of digital platforms on healthcare management. Their stories may underscore the advantages of timely access to health information, enhanced communication with healthcare providers, and the seamless coordination of care, highlighting the convenience and empowerment derived from utilizing electronic health records.

These narratives demonstrate the influence of perceived benefits in shaping individuals' attitudes and decisions regarding the privacy implications of EHRs. By prioritizing the positive outcomes and conveniences associated with electronic health records, individuals may minimize their concerns about potential privacy risks and security vulnerabilities. This narrative construction reflects the privacy calculus framework, where the perceived benefits of EHRs play a significant role in shaping individuals' attitudes and actions towards privacy.

The portrayal of EHRs as facilitators of efficient and personalized healthcare experiences may overshadow the apprehensions individuals have about the privacy and confidentiality of their health data. In doing so, the narrative construction of the perceived benefits of EHRs acts as a mechanism through which individuals rationalize and justify their acceptance and utilization of digital platforms for healthcare management.

To offer a thorough synopsis of the elements influencing the Privacy Paradox in EHRs and to clarify how Narrative Theory functions in understanding these elements, the summary table that follows is provided. The main concepts discussed in this paper are summarized in this table, which also shows how user behavior and decision-making regarding privacy in electronic health records are influenced by cognitive biases, awareness (or lack thereof), convenience prioritization, trust in healthcare systems or technology providers, and the balance of perceived

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

benefits against risks. The table also illustrates how narrative theory provides a sophisticated prism through which these processes can be comprehended, providing insights into the intricate interactions between specific behaviors and more general society narratives.

Table 1 : The Interplay of Factors Influencing the Privacy Paradox in EHRs Through the Lens of Narrative Theory

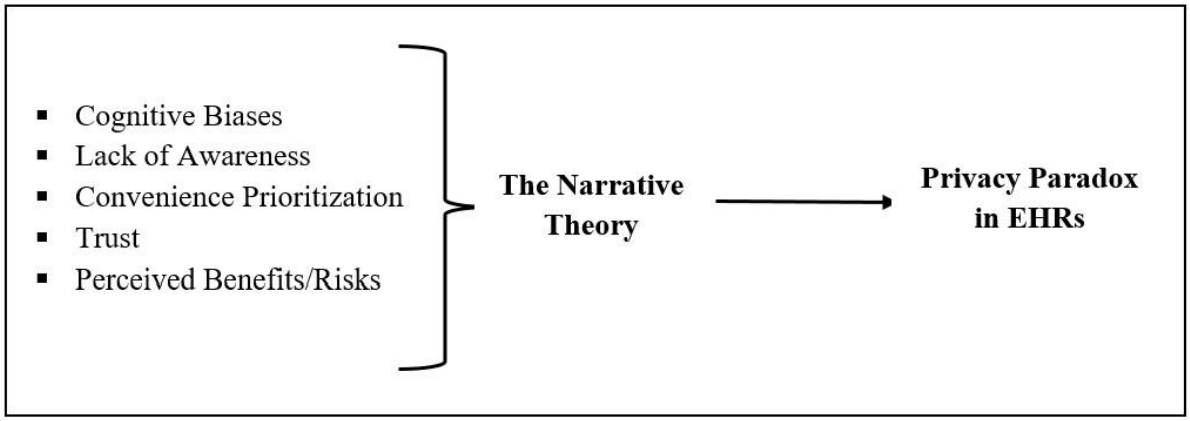
Factor	Description	Influence on Privacy Paradox	Role of Narrative Theory
Cognitive Biases	Systematic patterns of deviation from norm or rationality in judgment, leading to the privacy paradox.	Affects decision-making and perception of privacy risks.	Explains how personal stories and biases shape privacy concerns and behaviors.
Lack of Awareness or Understanding	Limited comprehension of the privacy risks associated with EHRs.	Contributes to underestimating the importance of privacy protection.	Highlights the need for narrative-driven education to enhance privacy awareness.
Convenience Prioritization	Preference for the ease of access and use of EHRs over privacy concerns.	Leads to neglect of privacy risks in favor of usability and access benefits.	Suggests narratives can reframe the trade-off between convenience and privacy, emphasizing informed decisions.
Trust in Healthcare Systems or Technology Providers	Trust affects willingness to engage with EHRs and share personal health data.	Affects the adoption of EHRs and willingness to share sensitive information.	Narratives about positive or negative experiences can significantly influence trust levels.
Perceived Benefits/Risks	Weighing the advantages of EHRs against potential privacy risks.	May lead to overlooking privacy concerns due to perceived benefits.	Narrative Theory can help in constructing balanced perspectives that consider both benefits and privacy risks.

Source : The Author

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Following is a contribution of a theoretical framework that sums up the main elements treated in this part where the listed factors (Cognitive Biases, Lack of Awareness, Convenience Prioritization, Trust, Perceived Benefits/Risks) are the variables or constructs, and "The Narrative Theory" is the mechanism through which these factors are presumed to influence the outcome, which is the "Privacy Paradox in EHRs."

Figure 1 : Theoretical framework



Source : The Author

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

5. Conclusion :

Adressing the Privacy Paradox in EHRs in the light of the Narrative Theory

The evident conclusion to be drawn from this paper is that the narrative theory provides a framework through which five valuable factors influence the occurrence of Privacy Paradoxe in EHRs. Narrative theory offers a more profound and sophisticated explanation for why individuals could behave in ways that run counter to their professed privacy concerns. It acknowledges how complicated human behavior can be and how storytelling may influence how we behave, especially when it comes to using technology.

Overall, this research supports the idea that, firstly, cognitive biases can be addressed in the context of EHR privacy concerns. By acknowledging the influence of cognitive biases such as optimism bias and confirmation bias, healthcare organizations and policymakers can develop targeted interventions to counteract these biases. Strategies may include providing accurate information about privacy risks, utilizing real-life scenarios to demonstrate potential consequences, and fostering critical thinking skills to mitigate the impact of cognitive biases on privacy decision-making.

Besides, addressing the lack of awareness or understanding of privacy risks in EHRs involves incorporating narrative-based educational initiatives. By contextualizing privacy risks within relatable narratives and real-world examples, individuals can learn more about the possible consequences of disclosing private health information electronically. Healthcare organizations can develop storytelling-based educational materials, interactive workshops, and engaging digital content to enhance individuals' awareness and comprehension of privacy risks associated with EHRs.

The narrative approach can also be utilized to reframe the trade-off between convenience and privacy concerns in the context of EHR adoption. By presenting narratives that highlight the value of privacy protection alongside the benefits of convenience, individuals can be encouraged to make more informed decisions that consider both aspects. Healthcare providers and technology developers can facilitate this by integrating privacy-centric narratives into their communication strategies, product design, and user interfaces, emphasizing the importance of privacy alongside the convenience of EHRs.

Also, building and maintaining trust in the healthcare system and technology providers requires a narrative-driven approach that highlights transparency, accountability, and reliability. Narrative-based communication strategies can be used to emphasize the trustworthiness of EHR systems and the commitment of healthcare organizations and technology providers to

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

safeguarding individual privacy. By integrating trustworthy narratives into organizational messaging, privacy policies, and user agreements, healthcare stakeholders can reinforce trust and allay concerns about privacy in EHRs.

And finally, addressing the perception of benefits outweighing risks involves shaping narratives that present a balanced perspective on the implications of utilizing EHRs. By incorporating real-life stories that depict both the advantages and potential drawbacks of electronic health records, individuals might gain a deeper comprehension of the consequences regarding privacy. Health professionals and technology experts can leverage narrative-based content to depict diverse scenarios, showcasing the benefits of EHRs while acknowledging and addressing the associated privacy risks.

In conclusion, leveraging narrative theory to address the privacy paradox in EHRs requires a strategic focus on cognitive biases, awareness building, prioritizing privacy, fostering trust, and shaping balanced narratives about the benefits and risks. By integrating narrative-driven strategies into privacy communication, education, and system design, healthcare organizations and technology providers can effectively navigate the privacy paradox and promote informed decision-making among individuals utilizing electronic health records.

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

REFERENCES

Barth, S., & Jong, M D D. (2017, November 1). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telematics and Informatics, 34(7), 1038-1058. HTTPS://DOI.ORG/10.1016/J.TELE.2017.04.013

Beard, L., Schein, R., Morra, D., Wilson, K., & Keelan, J. (2012, January 1). The challenges in making electronic health records accessible to patients : Table 1. Journal of the American Medical Informatics Association, 19(1), 116-120. HTTPS://DOI.ORG/10.1136/AMIAJNL-2011-000261

Caine, K., & Tierney, W M. (2014, December 6). Point and Counterpoint : Patient Control of Access to Data in Their Electronic Health Records. Journal of General Internal Medicine, 30(S1), 38-41. HTTPS://DOI.ORG/10.1007/S11606-014-3061-0

Campos-Castillo, C., & Anthony, D L. (2014, July 24). The double-edged sword of electronic health records : implications for patient disclosure. Journal of the American Medical Informatics Association, 22(e1), e130-e140. HTTPS://DOI.ORG/10.1136/AMIAJNL-2014-002804

Coorevits, P., Sundgren, M., Klein, G O., Bahr, A., Claerhout, B., Daniel, C., Dugas, M., Dupont, D., Schmidt, A., Singleton, P., Moor, G D., & Kalra, D. (2013, October 18). Electronic health records: new opportunities for clinical research. Journal of Internal Medicine, 274(6), 547-560. HTTPS://DOI.ORG/10.1111/JOIM.12119

Dhagarra, D., Goswami, M., & Kumar, G. (2020, September 1). Impact of Trust and Privacy Concerns on Technology Acceptance in Healthcare : An Indian Perspective. HTTPS://DOI.ORG/10.1016/J.IJMEDINF.2020.104164

Dienlin, T., & Trepte, S. (2014, July 31). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285-297. HTTPS://DOI.ORG/10.1002/EJSP.2049

Dienlin, T., Masur, P K., & Trepte, S. (2019, September 20). A Longitudinal Analysis of the Privacy Paradox. HTTPS://DOI.ORG/10.31235/OSF.IO/FM4H7

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Ektor, Arzoglou., Yki, Kortesniemi. (2023). Alternative Platforms and Privacy Paradox: A System Dynamics Analysis. Lecture Notes in Computer Science, doi : 10.1007/978-3-031-35995-8_12

Entzeridou, E., Markopoulou, E., & Mollaki, V. (2018, February 1). Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. International Journal of Medical Informatics, 110, 98-107. **HTTPS://DOI.ORG/10.1016/J.IJMEDINF.2017.12.004**

Gautam Pratiksha & Mohd. Dilshad Ansari & Surender Kumar Sharma, 2019. "Enhanced Security for Electronic Health Care Information Using Obfuscation and RSA Algorithm in Cloud Computing," International Journal of Information Security and Privacy (IJISP), IGI Global, vol. 13(1), pages 59-69, January.

Ghazvini, A., & Shukur, Z. (2013, January 1). Security Challenges and Success Factors of Electronic Healthcare System. **HTTPS://DOI.ORG/10.1016/J.PROTCY.2013.12.183**

Graves, S. (2013, January 1). Confidentiality, Electronic Health Records, and the Clinician. Perspectives in Biology and Medicine, 56(1), 105-125. **HTTPS://DOI.ORG/10.1353/PBM.2013.0003**

James, T L., Warkentin, M., & Collignon, S. (2015, December 1). A dual privacy decision model for online social networks. **HTTPS://DOI.ORG/10.1016/J.IM.2015.07.010**

Jensen, P., Jensen, L., & Brunak, S. (2012). Mining electronic health records : towards better research applications and clinical care. Nature Reviews Genetics, 13, 395-405. **HTTPS://DOI.ORG/10.1038/NRG3208**.

Keshta, I., & Odeh, A. (2021, July 1). Security and privacy of electronic health records: Concerns and challenges. **HTTPS://DOI.ORG/10.1016/J.EIJ.2020.07.003**

Kokolakis, S. (2017, January 1). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122-134. **HTTPS://DOI.ORG/10.1016/J.COSE.2015.07.002**

Langer, E J. (1975, August 1). The illusion of control.. Journal of Personality and Social Psychology, 32(2), 311-328. **HTTPS://DOI.ORG/10.1037/0022-3514.32.2.311**

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Langer, N., & Ribarich, M. (2008, December 12). Using Narratives in Healthcare Communication. Educational Gerontology, 35(1), 55-62. **HTTPS://DOI.ORG/10.1080/03601270802388930**

Li, Y. (2012, December 1). Theories in online information privacy research: A critical review and an integrated framework. Decision Support Systems, 54(1), 471-481. **HTTPS://DOI.ORG/10.1016/J.DSS.2012.06.010**

Lin, A., Chen, W., & Hong, J C. (2021, January 1). Electronic health record data mining for artificial intelligence healthcare. Elsevier eBooks, 133-150. **HTTPS://DOI.ORG/10.1016/B978-0-12-821259-2.00008-9**

Marco, Vassallo. (2019). The Privacy Paradox in the Big Data Era? No Thanks, We Are the E-People : The E-People in the Big Data Era. 9(3):32-47. doi: 10.4018/IJCBPL.2019070103

Miron-Scahtz, Talya, Glyn, Elwyn. (2011). To serve and protect? Electronic health records pose challenges for privacy, autonomy and person-centered medicine. the International Journal of Person-Centered Medicine, doi: 10.5750/IJPCM.V1I2.84

McKeeby, J W., & Coffey, P S. (2018, January 1). The Importance and Use of Electronic Health Records in Clinical Research. Elsevier eBooks, 687-702. **HTTPS://DOI.ORG/10.1016/B978-0-12-849905-4.00040-X**

Meingast, M., Roosta, T., & Sastry, S S. (2006, August 1). Security and Privacy Issues with Health Care Information Technology. **HTTPS://DOI.ORG/10.1109/IEMBS.2006.260060**

Perera, G., Holbrook, A., Thabane, L., Foster, G., & Willison, D J. (2011, February 1). Views on health information sharing and privacy from primary care practices using electronic medical records. International Journal of Medical Informatics, 80(2), 94-101. **HTTPS://DOI.ORG/10.1016/J.IJMEDINF.2010.11.005**

Petty, R E., & Cacioppo, J T. (1986, January 1). Intricacies of the Elaboration Likelihood Model. Springer eBooks, 197-216. **HTTPS://DOI.ORG/10.1007/978-1-4612-4964-1_8**

Philip, Fei, Wu. (2019). The privacy paradox in the context of online social networking : A self-identity perspective. Journal of the Association for Information Science and Technology, 70(3):207-217. doi : 10.1002/ASI.24113

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Seddon, J J M., & Currie, W L. (2013, December 1). Cloud computing and trans-border health data : Unpacking U.S. and EU healthcare regulation and compliance. Health Policy and Technology, 2(4), 229-241. **HTTPS://DOI.ORG/10.1016/J.HLPT.2013.09.003**

Shah, S M., & Khan, R A. (2020, January 1). Secondary Use of Electronic Health Record: Opportunities and Challenges. IEEE Access, 8, 136947-136965. **HTTPS://DOI.ORG/10.1109/ACCESS.2020.3011099**

Sharathkumar, S., & Jagadamba, G. (2017). Adaptive content-aware access control of EPR resource in a healthcare system. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 205-210. **HTTPS://DOI.ORG/10.1109/ICACCI.2017.8125841**.

Shariff, A., Green, J., & Jettinghoff, W. (2021). The Privacy Mismatch: Evolved Intuitions in a Digital World. Current Directions in Psychological Science, 30, 159 - 166. **HTTPS://DOI.ORG/10.1177/0963721421990355**

Shen, N., Bernier, T., Sequeira, L., Strauss, J S., Silver, M P., Carter-Langford, A., & Wiljer, D. (2019, May 1). Understanding the patient privacy perspective on health information exchange: A systematic review. International Journal of Medical Informatics, 125, 1-12. **HTTPS://DOI.ORG/10.1016/J.IJMEDINF.2019.01.014**

Shih, H., & Liu, W. (2023, January 25). Beyond the trade-offs on Facebook : the underlying mechanisms of privacy choices. **HTTPS://DOI.ORG/10.1007/S10257-023-00622-6**

Sundar, S S., Kim, J., Rosson, M B., & Molina, M D M. (2020, April 21). Online Privacy Heuristics that Predict Information Disclosure. **HTTPS://DOI.ORG/10.1145/3313831.3376854**

Tobias, Dienlin., Philipp, K., Masur., Sabine, Trepte. (2021). A longitudinal analysis of the privacy paradox. New Media & Society, doi : 10.1177/14614448211016316

Tversky, A., & Kahneman, D. (1982, April 30). Judgment under uncertainty : Heuristics and biases. Cambridge University Press eBooks, 3-20. **HTTPS://DOI.ORG/10.1017/CBO9780511809477.002**

Vincenzo, Sanguineti. (2022). Narrative Theory. The International Encyclopedia of Health Communication, 1-5. doi: 10.1002/9781119678816.iehc0716

African Scientific Journal
ISSN : 2658-9311
Vol : 3, Numéro 22, Février 2024

Waldman, A E. (2020, February 1). Cognitive biases, dark patterns, and the 'privacy paradox'. Current Opinion in Psychology, 31, 105-109. **HTTPS://DOI.ORG/10.1016/J.COPSYC.2019.08.025**

Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017, March 1). Research issues for privacy and security of electronic health services. Future Generation Computer Systems, 68, 1-13. **HTTPS://DOI.ORG/10.1016/J.FUTURE.2016.08.011**