International Journal of Computer Applications Technology and Research
Volume 13–Issue 11, 18 – 24, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1311.1003

Security and Privacy Considerations in Voice Assistant Data Entry Systems for Healthcare Providers

Okeke Ogochukwu C.
Department of Computer Science
Chukwuemeka Odumegwu Ojukwu University Uli Anambra State, Nigeria

Ezenwegbu Nnamdi Chimaobi
Department of Computer Science
Chukwuemeka Odumegwu Ojukwu University Uli Anambra State, Nigeria

Abstract: Voice assistants are increasingly being integrated into healthcare environments for data entry, enhancing efficiency and accessibility for healthcare providers. However, using these systems raises critical security and privacy concerns due to the sensitive nature of health data and the unique vulnerabilities of voice-enabled technologies. This paper examines the security and privacy implications of using voice assistants for data entry in healthcare settings, exploring risks associated with data interception, unauthorized access, and inadvertent information leakage. We analyze how voice assistant systems process, store, and transmit data, identifying potential attack vectors and privacy vulnerabilities. The paper also reviews existing regulations and standards, such as HIPAA, that impact the deployment of voice-enabled systems in healthcare. To address these challenges, we propose a framework for secure voice data entry, incorporating multi-layered authentication, encryption, and real-time anomaly detection. Our findings underscore the need for healthcare providers to adopt robust security protocols and privacy practices to ensure compliance and protect patient confidentiality. This research contributes to a growing body of knowledge aimed at the safe and ethical integration of voice assistants in healthcare, providing guidelines for technology developers and healthcare administrators.

Keywords: Voice Assistants, Healthcare Data Security, Patient Privacy, Data Entry Systems, HIPAA Compliance, Voice Recognition Vulnerabilities, Healthcare Technology, Privacy Frameworks

1. INTRODUCTION

Voice assistants (VAs) are gaining traction in healthcare as they offer hands-free, voice-controlled data entry solutions that can significantly enhance workflow efficiency and improve patient interaction (Kumah-Crystal et al., 2018). These systems are especially advantageous in clinical settings where direct physical interaction with devices can be challenging, such as in sterile environments, where touchless interfaces can aid infection control (Darda et al., 2021). For instance, using VAs to capture patient data or dictate notes can streamline clinical tasks and free up time for healthcare providers to focus on patient care (Blijleven et al., 2022). However, the sensitive nature of healthcare data necessitates a careful approach to integrating VAs, as their usage raises potential security and privacy concerns. These concerns are particularly critical due to the regulatory frameworks that govern health data, including the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which mandates strict protection of patient information (Centers for Medicare & Medicaid Services, n.d.).

Several factors complicate the secure implementation of VAs in healthcare. Firstly, VAs typically rely on cloud processing for data interpretation and storage, which involves transmitting voice data to external servers. This process introduces security vulnerabilities, such as the potential for unauthorized access or data interception during transmission (Gupta, 2022; Bălan, 2023). Further, recent studies highlight vulnerabilities in voice recognition systems, such as susceptibility to voice replay attacks, which allow malicious actors to access VA-controlled systems using recorded voice samples (Seymour et al., 2023). Such attacks can have serious implications when sensitive patient information is stored or processed through VAs, exposing healthcare systems to data breaches and regulatory violations.

The complexity of integrating VAs into healthcare also arises from the need to maintain strict compliance with data protection standards. Electronic Health Records (EHR) systems, for example, are required to provide high levels of data integrity and access control. Yet, VAs, due to their continuous listening features, can inadvertently capture unauthorized data, potentially leading to breaches of patient privacy (Blijleven et al., 2022; Centers for Medicare & Medicaid Services, n.d.). Additionally, the ability of VAs to process and store data in the cloud raises questions about data ownership and control, which are crucial for ensuring compliance with privacy laws and healthcare standards (Sezgin et al., 2021).

This paper explores the security and privacy challenges associated with VA data entry systems in healthcare, with a particular focus on the regulatory and technical hurdles that impact their safe adoption. We provide an analysis of potential vulnerabilities in VA systems, evaluate the gaps in regulatory compliance, and propose a framework for implementing secure and privacy-preserving VA solutions in healthcare. By addressing these challenges, this research aims to support healthcare providers and technology developers in creating more secure, efficient, and compliant VA systems.

2. SECURITY AND PRIVACY CHALLENGES

The rapid adoption of VAs in healthcare is accompanied by several technical and regulatory challenges. Most VA systems rely on cloud processing for data interpretation and storage, necessitating the transfer of sensitive patient data across networks that may be vulnerable to interception or unauthorized access (Gupta, 2022; Bălan, 2023). Moreover, privacy concerns arise due to the continuous listening features of many VAs, which can result in accidental data capture and potential regulatory violations. This paper explores the various security and privacy risks associated with VAs in healthcare, evaluates the compliance challenges posed by voice-enabled data entry, and proposes a security framework to mitigate these risks.

Diverse attacks: Voice assistants (VAs) are intricate systems composed of multiple software and hardware elements, which results in a wide array of vulnerabilities and threat vectors. This

diversity in potential threats complicates the process of systematically identifying and addressing security risks. For instance, adversaries can craft adversarial inputs that, while sounding harmless to human listeners, are interpreted as harmful commands by the VA's speech recognition software (Kumah-Crystal et al., 2018). Additionally, attackers might develop a malicious third-party application that, due to errors in natural language processing, could be unintentionally activated by users (Seymour et al., 2023). Hardware vulnerabilities also pose risks, as attackers can utilize ultrasonic waves (Darda et al., 2021), laser (Blijleven et al., 2022), or electromagnetic interference (Gupta, 2022) to inject imperceptible commands, exploiting the VA's sensor inputs to execute unintended actions.

Stand-alone defences: Most current defense mechanisms are designed to counter specific types of attacks in isolation. For instance, liveness detection methods are primarily employed to identify and block voice spoofing attempts (Sezgin et al., 2021), while adversarial training focuses solely on mitigating attacks that exploit adversarial examples (Kumah-Crystal et al., 2018). However, there is limited understanding of how these security measures would function within the more complex, multi-threat landscape that VAs face, including factors like cost of implementation, usability, and overall security efficacy (Gupta, 2022). While numerous studies suggest effective results, VA developers continue to encounter difficulties in selecting and implementing the most suitable protective strategies for comprehensive security.

Lack of systematic perspectives: Numerous studies focus solely on individual components of a VA, such as speech recognition or speaker verification, rather than examining the VA system as a whole, and often without considering a VA-specific context. For example, much of the research on attacks (Kumah-Crystal et al., 2018; Darda et al., 2021) and defences (Seymour et al., 2023) relevant to the security of speech recognition—the central feature of a VA—tends to evaluate standalone models that are not yet implemented in commercial voice assistants. Although these studies are not always labelled under VA-specific terms, their findings may become applicable to voice assistant technology in the future and thus warrant careful consideration.

Backdoor Attack: Backdoor attacks are a prevalent threat to automatic speech recognition (ASR) models, where attackers embed subtle, inaudible signals within audio data—such as music clips or voicemails—to alter how the model processes this data. These attacks introduce a specific input, known as a trigger, that manipulates the model into executing the attacker's desired response. Concealed commands within adversarial audio can be transformed into the attacker's intended instructions through the VA's neural processing, rendering hidden directives audible to the system but often imperceptible to human listeners. Kasher et al. demonstrated how backdoor systems could control smart devices through voice commands, using adversarial audio perturbations embedded within music-only audio to convert these into actionable commands for the VA (Seymour et al., 2023). This approach maximizes impact by using varied base vectors, targeted phrases, and degrees of perturbation strength, making it possible to modify both musical and speech samples effectively. Although selecting the correct target phrase is crucial, backdoor attacks can achieve transcription accuracy rates exceeding 50%, ensuring the successful transmission of specific commands (Kumah-Crystal et al., 2018).

Unauthorized Data Access: One of the most critical security risks associated with VAs in healthcare is unauthorized access to sensitive data. VAs often rely on cloud servers for processing voice commands, requiring data to be transmitted over potentially unsecured networks (Gupta, 2022). This reliance on cloud-based systems introduces vulnerabilities that can be exploited by malicious actors to intercept or manipulate data during transmission. Unauthorized access to healthcare data poses a substantial risk, as patient information is highly sensitive and subject to regulatory oversight (Centers for Medicare & Medicaid Services, n.d.).

Voice Replay Attacks: VAs are also susceptible to voice replay attacks, where attackers use recorded voice samples to access the system fraudulently (Seymour et al., 2023). In healthcare, such attacks could lead to unauthorized access to EHRs, compromising patient confidentiality and trust. Voice recognition systems in healthcare VAs must incorporate advanced authentication mechanisms to minimize these risks.

Continuous Listening: Many VAs utilize continuous listening features, which increase the likelihood of accidental data capture. This raises significant privacy concerns in healthcare, where even inadvertent capture of patient conversations could constitute a violation of privacy regulations, such as HIPAA (Darda et al., 2021). Continuous listening without adequate security safeguards could expose sensitive patient information and lead to unintended disclosures (Sezgin et al., 2021).

Regulatory Compliance Challenges: Compliance with healthcare regulations, particularly HIPAA, mandates stringent data protection measures for any system handling patient information. However, VA systems pose compliance challenges due to the ambiguity surrounding data storage, ownership, and access control (Centers for Medicare & Medicaid Services, n.d.). Ensuring that VAs meet regulatory standards requires implementing strict data management protocols, especially for cloud-based processing and storage (Kumah-Crystal et al., 2018).

3. LITERATURE REVIEW

Voice assistants (VAs) have undergone significant advancements in recent years, becoming essential in various fields for improving user interaction and automating tasks (Bălan, 2023). In healthcare, VAs allow providers to manage patient records more efficiently, which is increasingly important as electronic health records (EHR) are adopted as the industry standard for patient data management (Centers for Medicare & Medicaid Services, n.d.). However, unlike traditional data entry methods, VAs introduce distinct security challenges due to their reliance on voice recognition technology, making them susceptible to attacks such as voice replay and unauthorized access (Seymour et al., 2023). Furthermore, the cloud-based infrastructure commonly employed by VAs creates additional complications regarding data ownership and control, both critical for ensuring HIPAA compliance and protecting sensitive healthcare information (Sezgin et al., 2021).

Research highlights several benefits of VAs in healthcare, including improvements in workflow efficiency and patient satisfaction, as VAs enable hands-free interaction and rapid data retrieval (Kumah-Crystal et al., 2018). However, these benefits are tempered by concerns over security and privacy, as the continuous listening feature of many VAs increases the risk of inadvertently capturing sensitive information, potentially

leading to privacy violations and regulatory issues (Darda et al., 2021). The unique security and privacy concerns associated with VAs underscore the pressing need for robust protection mechanisms and strict adherence to data security standards in healthcare settings (Blijleven et al., 2022). This review emphasizes the necessity of enhanced security strategies specifically tailored to voice-based systems in healthcare to mitigate the inherent risks and ensure compliance with privacy regulations.

3.1 Regulatory and Standards Review for Voice-Enabled Systems in Healthcare

The deployment of voice-enabled systems (VES) in healthcare is influenced by several regulations and standards aimed at safeguarding patient information and ensuring system security. Among these, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, as well as international standards like the General Data Protection Regulation (GDPR) and specific healthcare IT guidelines, play crucial roles.

3.1.1 Health Insurance Portability and Accountability Act (HIPAA)

HIPAA establishes a set of federal standards for the protection of "Protected Health Information" (PHI), which includes any data that can identify a patient and relates to their health condition, treatment, or payment information. Voice-enabled systems processing PHI must adhere to HIPAA guidelines, which mandate:

a) Privacy Rule: VES in healthcare must safeguard PHI by limiting unauthorized access and ensuring confidentiality. Voice assistants, which continuously process spoken data, must have mechanisms to prevent unintentional recording and restrict access to authorized personnel only (Centers for Medicare & Medicaid Services, n.d.).
b) Security Rule: This rule requires that VES implement safeguards for data integrity and confidentiality. These safeguards include administrative, physical, and technical measures to prevent breaches. End-to-end encryption, secure data storage, and restricted user access are critical for VES compliance under HIPAA (Kumah-Crystal et al., 2018).
c) Breach Notification Rule: In the event of a data breach, HIPAA mandates that healthcare providers notify affected patients, the U.S. Department of Health and Human Services (HHS), and sometimes the media, depending on the breach's scope. Voice-enabled systems, vulnerable to cyberattacks such as data interception or unauthorized access, must have measures to detect and report breaches swiftly.

3.1.2 General Data Protection Regulation (GDPR)

For healthcare providers in the European Union or those serving EU citizens, GDPR imposes stringent data protection requirements. GDPR emphasizes the patient's right to privacy and control over personal data:

a) Data Minimization and Purpose Limitation: Voice-enabled systems in healthcare must ensure that only essential data is captured and that it is used strictly for the stated purpose. Continuous voice listening, for example, must be minimized or anonymized when feasible to comply with GDPR's data minimization principle (Sezgin et al., 2021).
b) Data Subject Rights: GDPR grants patients the right to access, correct, or delete their data, which can be complex in voice-enabled systems where audio data might be stored across cloud servers. Compliance with these rights requires clear processes for data retrieval and erasure.
c) Data Security and Accountability: GDPR requires VES to demonstrate data security practices and conduct risk assessments. Regular audits, clear accountability for data handling, and the use of data encryption are essential to meet GDPR's requirements.

3.1.3 NIST Standards for Secure Voice-Enabled Systems

The National Institute of Standards and Technology (NIST) offers guidelines on implementing secure and privacy-aware digital technologies, including VES. NIST's standards are not legally binding but serve as a benchmark for best practices:

a) SP 800-53 and SP 800-63 Guidelines: These publications provide a framework for access control, secure authentication, and data protection, which are highly relevant to voice systems processing healthcare data. For example, multi-factor authentication (MFA) and encryption are recommended to enhance security in voice data systems (Gupta, 2022).
b) Real-Time Monitoring and Anomaly Detection: NIST standards advocate for real-time monitoring to detect and respond to unusual activity patterns, which is critical for voice assistants in healthcare to prevent unauthorized access or inadvertent data sharing (Blijleven et al., 2022).

3.1.4 HITRUST Certification

The Health Information Trust Alliance (HITRUST) certification is a widely accepted framework for managing security, privacy, and compliance risk in healthcare. HITRUST certification aligns with both HIPAA and GDPR and ensures that systems meet rigorous standards for data protection:

Risk Management and Assessment: HITRUST requires regular assessments to evaluate risk exposure, focusing on incident response and secure data management. Voice-enabled systems in healthcare can leverage HITRUST certification as a pathway to demonstrate compliance with multiple regulatory standards.

Continuous Improvement in Security Protocols: HITRUST promotes the ongoing enhancement of security protocols, making it essential for VES to adopt adaptive security measures in response to emerging threats, especially as voice-enabled technology evolves.

3.1.5 ISO/IEC 27001

The ISO/IEC 27001 is an international standard for information security management systems (ISMS), widely applicable to healthcare data systems, including voice-enabled technology.

ISO/IEC 27001 emphasizes structured risk management, which is beneficial for healthcare providers deploying VES:

a) ISMS Framework Implementation: An ISMS framework provides a structured approach to managing sensitive information. VES that adhere to ISO/IEC 27001's ISMS principles will have clear security policies and procedures for handling PHI and mitigating risks (Bălan, 2023).
b) Compliance and Regular Audits: ISO/IEC 27001 requires periodic audits and reviews, which help ensure ongoing compliance with information security policies. Voice-enabled healthcare systems can utilize this standard to uphold high levels of data protection and system resilience.

Voice-enabled systems in healthcare must navigate a complex landscape of regulations and standards, including HIPAA, GDPR, NIST guidelines, HITRUST, and ISO/IEC 27001. These frameworks collectively emphasize the importance of data privacy, security, and accountability, making it crucial for VES to implement multi-layered protection measures, from encryption to real-time monitoring. Compliance with these regulations ensures that VES can offer healthcare providers both operational efficiency and robust patient data protection, helping to maintain trust and meet regulatory obligations.

4. PROPOSED SECURITY FRAMEWORK FOR VOICE ASSISTANT SYSTEMS

In light of the discussed security and privacy challenges, this paper proposes a security framework aimed at reducing risks associated with VAs in healthcare environments. The framework includes elements such as multi-layered authentication, end-to-end encryption, real-time anomaly detection, and privacy safeguards for continuous listening.

Multi-Layered Authentication: To prevent unauthorized access and voice replay attacks, healthcare VAs should employ multi-layered authentication. This could integrate voice biometrics, PIN verification, or device-based authentication to restrict access to patient data strictly to authorized users (Sezgin et al., 2021). Such a layered approach ensures robust protection against unauthorized attempts to access sensitive healthcare information (Seymour et al., 2023).

End-to-End Encryption: Data transmitted between the VA device and cloud servers should be secured using end-to-end encryption, preventing interception and safeguarding patient data from unauthorized access (Bălan, 2023). Applying encryption throughout multiple stages of data processing is essential to ensure comprehensive protection against data breaches and uphold privacy standards (Gupta, 2022).

Real-Time Anomaly Detection: Real-time monitoring and anomaly detection systems are valuable for identifying unusual access patterns or unexpected voice activity. These systems allow healthcare providers to detect potential security breaches promptly, enabling intervention before substantial harm occurs (Blijleven et al., 2022). Early detection of anomalies helps maintain the integrity and confidentiality of healthcare data within VA systems.

Privacy Safeguards for Continuous Listening: To mitigate privacy risks associated with continuous listening, healthcare VAs should offer privacy settings that allow users to deactivate or limit the listening capabilities as needed. These controls reduce the likelihood of unintentional data capture, lowering the risk of privacy infringements (Darda et al., 2021). Furthermore, establishing voice data retention policies ensures that sensitive information is only stored for as long as necessary, in compliance with privacy regulations (Kumah-Crystal et al., 2018).

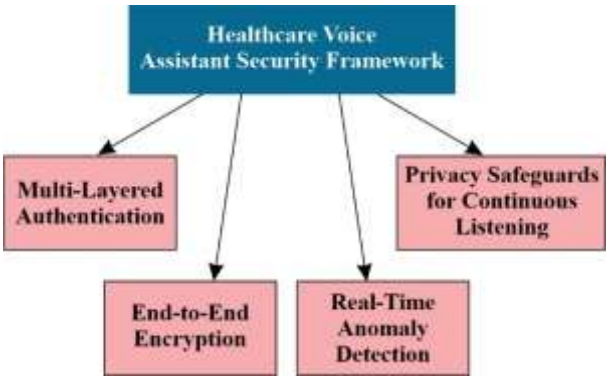

Figure 1: Security framework for voice assistant systems in healthcare

5. DISCUSSION

The integration of voice assistants (VAs) in healthcare offers significant advantages, such as improving workflow efficiency and reducing the manual burden of data entry, thereby allowing healthcare professionals to focus more on patient care (Kumah-Crystal et al., 2018). However, these benefits come with considerable security and privacy concerns that need careful mitigation to ensure safe usage in healthcare settings (Seymour et al., 2023). A robust, multi-layered security framework, like the one proposed in this study, is essential to address these risks while preserving the operational advantages VAs provide.

5.1 Key Security and Privacy Considerations for VAs in Healthcare

A structured security framework for VAs should include multi-layered authentication, encryption, and real-time anomaly detection. Each of these components contributes to securing VAs for healthcare applications, where they handle sensitive patient data and must comply with stringent privacy standards such as HIPAA. The following table summarizes these components, highlighting the specific challenges each component addresses and the best practices associated with each

Table 1: Key security and privacy components

Security Component	Challenge Addressed	Best Practices	Supporting Sources
Multi-Layered Authentication	Unauthorized access and voice replay attacks	Use voice biometrics, PINs, or device-based authentication to restrict access strictly to authorized individuals.	Sezgin et al. (2021); Seymour et al. (2023)
End-to-End Encryption	Data interception during transmission	Encrypt data throughout its lifecycle, including during transmission between VAs and cloud servers, to protect patient information from interception and unauthorized access.	Gupta (2022); Bălan (2023)
Real-Time Anomaly Detection	Early identification of security breaches	Deploy real-time monitoring systems to detect unusual access patterns or unauthorized voice activity, allowing healthcare providers to intervene before significant damage occurs.	Blijleven et al. (2022)
Privacy Safeguards for Continuous Listening	Inadvertent data capture and privacy breaches	Limit continuous listening features and implement data retention policies to ensure that only essential data is stored and for a defined period, complying with regulatory standards.	Centers for Medicare & Medicaid Services (n.d.); Darda et al. (2021)

5.2 Addressing Compliance Challenges through Privacy Safeguards

Compliance with regulations such as HIPAA in the U.S. and GDPR in Europe requires specific privacy measures, which are especially critical for VAs due to their continuous listening and data-processing capabilities (Centers for Medicare & Medicaid Services, n.d.). Limiting continuous listening functions can minimize accidental capture of sensitive data, aligning with privacy principles like data minimization. Additionally, data retention policies that enforce the secure deletion of voice recordings after a predefined period can prevent potential breaches and enhance trust among patients (Sezgin et al., 2021).

The structured framework proposed here enables healthcare providers to leverage VAs while aligning with regulatory requirements. By implementing these privacy and security safeguards, healthcare facilities can not only meet legal standards but also protect patient confidentiality and trust, which are foundational to the effective use of VAs in medical environments.

6. CONCLUSION

The deployment of voice assistants (VAs) in healthcare presents both valuable opportunities and significant security and privacy challenges. VAs have the potential to streamline healthcare workflows, reduce administrative burdens, and improve patient-provider interactions by allowing hands-free data entry and real-time information access. However, these benefits come with risks associated with unauthorized access, data interception, and inadvertent data capture due to continuous listening features. To address these issues, this paper proposed a comprehensive security framework, including multi-layered authentication, end-to-end encryption, real-time anomaly detection, and privacy safeguards tailored for VAs in healthcare.

Implementing this framework enables healthcare providers to navigate the complex regulatory landscape, adhering to standards such as HIPAA and GDPR, while effectively protecting patient information. Adopting privacy-focused practices such as data minimization and limiting continuous listening functions helps align VAs with regulatory requirements, enhancing trust and ensuring compliance. This research highlights the necessity of robust security and privacy mechanisms to facilitate the safe adoption of VAs in healthcare, paving the way for innovative solutions that respect patient confidentiality and uphold data protection standards. Future research should continue to refine these security strategies and explore emerging technologies that can further secure VAs, ultimately supporting safer, more efficient healthcare delivery.

6. REFERENCES

[1] Apple (2018) iOS – Siri – Apple (UK). Available at: https://www.apple.com/uk/ios/siri/. (Accessed: 15 December 2023).

[2] Bălan, C. (2023). Chatbots and Voice Assistants: Digital Transformers of the Company–Customer Interface—*A Systematic Review of the Business*

Research Literature. Journal of Theoretical and Applied Electronic Commerce Research, 18(2), 995. https://doi.org/10.3390/jtaer18020051

[3] Bhatt, V. N. (2020). *Alexa for Health Practitioners* (Order No. 27835534). Available from ProQuest One Academic. (2409092166). http://ezproxy.newcastle.edu.au/login?url=https://www.proquest.com/dissertations-theses/alexa-health-practitioners/docview/2409092166/se-2

[4] Blijleven, V., Hoxha, F., & Jaspers, M. (2022). Workarounds in Electronic Health Record Systems and the Revised Sociotechnical Electronic Health Record Workaround Analysis Framework: Scoping Review. Journal of Medical Internet Research, https://doi.org/10.2196/33046

[5] Buoy Health (2018) Buoy Health: Check Symptoms & Find the Right Care. Available at: https://www.buoyhealth.com/. (Accessed: 25 November 2023).

[6] Centers for Medicare & Medicaid Services. (n.d.). *Electronic Health Records* https://www.cms.gov/priorities/key-initiatives/e-health/records#:~:text=An%20Electronic%20Health%20Record%20(EHR,progress%20notes%2C%20problems%2C%20medications%2C

[7] Complexity. (2023). Retracted: English Phrase Speech Recognition Based on Continuous Speech Recognition Algorithm and Word Tree Constraints. *Complexity, 2023* https://doi.org/10.1155/2023/9892303

[8] Darda, P., Nerlekar, V., Bairagi, U., Pendse, M., & Sharma, M. (2021). Usage of Voice Assistant in Time of Covid-19 as a Touchless Interface. *Academy of Strategic Management Journal, Suppl.Special Issue 6, 20,* 1-13. Retrieved from http://ezproxy.newcastle.edu.au/login?url=https://www.proquest.com/scholarly-journals/usage-voice-assistant-time-covid-19-as-touchless/docview/2599946778/se-2

[9] Google (2018) Google Assistant – Your Own Personal Google. Available at: https://assistant.google.com/intl/en_uk/. (Accessed: 15 December 2023).

[10] Google Cloud (2018) Cloud Speech-to-Text - Speech Recognition | Cloud Speech-to-Text API | Google Cloud. Available at: https://cloud.google.com/speech-to-text. (Accessed: 28 November 2024).

[11] Goss, F., Zhou, L., Weiner, S. (2016) 'Incidence of Speech Recognition Errors in the Emergency Department', International Journal of Medical Informatics, vol.93, pp.70-73. DOI: 10.1016/j.ijmedinf.2016.05.005.

[12] Gupta, H. (2022). Re-Modelling the Hospitality Business Using Artificial Intelligence as a Strategic Tool. *Johar, 17(2),* 1-16. http://ezproxy.newcastle.edu.au/login?url=https://www.proquest.com/scholarly-journals/re-modelling-hospitality-business-using/docview/2833745570/se-2

[13] Herff, C., Schultz, T. (2016) 'Automatic Speech Recognition from Neural Signals: A Focused Review', Frontiers in Neuroscience, vol.10, p.429. DOI: 10.3389/fnins.2016.00429.

[14] Kazuhiro, N., & Tomoaki, K. (2017). Psychologically-Inspired Audio-Visual Speech Recognition Using Coarse Speech Recognition and Missing Feature Theory. Journal of Robotics and Mechatronics, 29(1), 105-113. https://doi.org/10.20965/jrm.2017.p0105

[15] Kumah-Crystal, Y. A., Pirtle, C. J., Whyte, H. M., Goode, E. S., Anders, S. H., & Lehmann, C. U. (2018). Electronic Health Record Interactions through Voice: A Review. *Applied clinical informatics, 9(3), 541–552.* https://doi-org.ezproxy.newcastle.edu.au/10.1055/s-0038-1666844

[16] Kumar, M., & Mostafa, J. (2020). Electronic health records for better health in the lower- and middle-income countries: A landscape study. [Electronic health records for better health] Library Hi Tech, 38(4), 751-767. https://doi.org/10.1108/LHT-09-2019-0179

[17] Liu, J., Wan, F., Zou, J., & Zhang, J. (2023). Exploring factors affecting People's willingness to use a voice-based in-car assistant in electric cars: An empirical study. World Electric Vehicle Journal, 14(3), 73. doi:https://doi.org/10.3390/wevj14030073

[18] Matyunina, J. (2017) 'AI in Mobile Apps: How to Make an App Like Siri', Codetiburon. Available at: https://codetiburon.com/ai-mobile-apps-make-app-like-siri/. (Accessed: 29 June 2018).

[19] MedWhat (2018) MedWhat | Your virtual medical assistant. Available at: https://medwhat.com/. (Accessed: 25 November 2023).

[20] Meffen, A., Sayers, R. D., Gillies, C. L., Khunti, K., & Gray, L. J. (2022). Are major lower extremity amputations well recorded in primary care electronic health records?: Insights from primary care electronic health records in England. *Primary Health Care Research & Development, 23* doi:https://doi.org/10.1017/S1463423622000718

[21] Miller, J. (2020) 'Self-Diagnosis on Internet not Always Good Practice', The Harvard Gazette. Available at: https://news.harvard.edu/gazette/story/2020/07/self-diagnosis-on-internet-not-good-practice/. (Accessed: 26 August 2023).

[22] Park, J., Amendah, E., Lee, Y., & Hyun, H. (2019). M-payment service: Interplay of perceived risk, benefit, and trust in service adoption. *Human Factors and Ergonomics in Manufacturing & Service Industries, 29(1),* 31–43.

[23] Poder, T., Fisette, J., Dery, V. (2018) 'Speech Recognition for Medical Dictation: Overview in Quebec and Systematic Review', Journal of Medical Systems, 42(5), pp.1-8. DOI: 10.1007/s10916-018-0947-0.

[24] Sense.ly Corporation (2018) Ask NHS – Virtual Assistant. (Version 3.0.2) [Mobile app]. Available at:

iTunes Store & Google Play (Downloaded: 25 December 2023).

[25] Sensely (2018) Sensely – How are you feeling today?. Available at: ttp://www.sensely.com/. (Accessed: 25 December 2023).

[26] Seymour, W., Zhan, X., Cote, M., & Such, J. (2023). *A systematic review of ethical concerns with voice assistants. Ithaca:* Cornell University Library, arXiv.org. doi:https://doi.org/10.1145/3600211.3604679

[27] Sezgin, E., Noritz, G., Lin, S., & Huang, Y. (2021). Feasibility of a Voice-Enabled Medical Diary App (SpeakHealth) for Caregivers of Children With Special Health Care Needs and Health Care Providers: Mixed Methods Study. JMIR Formative Research, 5(5)https://doi.org/10.2196/25503

[28] Snyder, E. C., Mendu, S., Sundar, S. S., & Abdullah, S. (2023). Busting the one-voice-fits-all myth: Effects of similarity and customization of voice-assistant personality. International Journal of Human-Computer Studies, 180, 1-13. doi:https://doi.org/10.1016/j.ijhcs.2023.103126

[29] Syam, N. & Sharma, A. (2018). *Waiting for a sales renaissance in the fourth industrial revolution: machine learning and artificial intelligence in sales research and practice, Indus*. Mark. Manag. 69, 135–146.

[30] Thiago H O da, S., Furtado, V., Furtado, E., Mendes, M., Almeida, V., & Sales, L. (2024). How Do Illiterate People Interact with an Intelligent Voice Assistant? International Journal of Human - Computer Interaction, 40(3), 584-602. https://doi.org/10.1080/10447318.2022.2121219

[31] Wen-Chin, H., & Mu-Heng, L. (2023). Semantic technology and anthropomorphism: Exploring the impacts of voice assistant personality on user trust, perceived risk, and attitude. *Journal of Global Information Management, 31*(1), 1-21. doi:https://doi.org/10.4018/JGIM.318661

[32] You, C. & Ma, B. (2017) 'Spectral-Domain Speech Enhancement for Speech Recognition', Speech Communication, vol.94, pp.30-41. DOI: 10.1016/j.specom.2017.08.007.

[33] Your.MD AS (2017) Your.MD – Health Guide. (Version 2.8.4) [Mobile app]. Available at: iTunes App Store & Google Play (Downloaded: 25 November 2023).