How to Cite:
Alshammari, M. F. N., Alrshidi, A. S. M., Alrasheidi, B. M. H., Alsudais, A. S. A., Alghadeer, S. O. A., Alshammari, N. M. M., Alshammari, H. M. N., Aleiid, A. S., Alsayyari, A. M., Alharbi, A. J. M., & Almutairi, F. M. H. (2024). Biometric devices in health management: Pharmacists' contribution to data interpretation and patient guidance. *International Journal of Health Sciences*, *8*(S1), 1423–1433. https://doi.org/10.53730/ijhs.v8nS1.15261

Biometric devices in health management: Pharmacists' contribution to data interpretation and patient guidance

Mansour Fahad Nasser Alshammari
KSA, National Guard Health Affairs

Ahmed Saleh Madws Alrshidi
KSA, National Guard Health Affairs

Bander Mohammad Haia Alrasheidi
KSA, National Guard Health Affairs

Abdullah Sulaiman Abdullah Alsudais
KSA, National Guard Health Affairs

Saleh Obaid Abdullah Alghadeer
KSA, National Guard Health Affairs

Nezar Mohammad Mutlaq Alshammari
KSA, National Guard Health Affairs

Hassan Mashe Noman Alshammari
KSA, National Guard Health Affairs

Alaa Saud Aleiid
KSA, National Guard Health Affairs

Alaa Musaad Alsayyari
KSA, National Guard Health Affairs

Abdullah Jatil Mohammed Alharbi
KSA, National Guard Health Affairs

Fayez Mohammed Hubayni Almutairi
KSA, National Guard Health Affairs

International Journal of Health Sciences E-ISSN 2550-696X © 2024.
Corresponding email: *akk29337@gmail.com*
Manuscript submitted: 01 Jan 2024, Manuscript revised: 09 Jan 2024, Accepted for publication: 15 Jan 2024

***Abstract*---Background:** The rapid advancement of biometric technology in health management has opened new avenues for patient identification and data security. As healthcare systems increasingly adopt biometric devices, there is a growing need for healthcare professionals, particularly pharmacists, to interpret biometric data effectively. **Aim:** This study aims to explore the role of pharmacists in utilizing biometric devices for health management, emphasizing their contribution to data interpretation and patient guidance. **Methods:** A comprehensive literature review was conducted, analyzing various studies on biometric devices in healthcare and the involvement of pharmacists. The research focused on the types of biometric technologies utilized, the responsibilities of pharmacists, and case studies highlighting successful implementations. **Results:** The findings reveal that pharmacists play a crucial role in interpreting biometric data, educating patients on its implications, and ensuring adherence to medication regimens. They also assist in managing chronic diseases through continuous monitoring enabled by biometric devices. Furthermore, pharmacists facilitate patient engagement by promoting the understanding and acceptance of biometric technologies. **Conclusion:** As biometric devices become integral to health management, pharmacists are well-positioned to lead in data interpretation and patient education. Their involvement enhances patient safety, optimizes therapeutic outcomes, and fosters a more comprehensive approach to healthcare delivery. Future research should focus on developing standardized protocols for pharmacists' training in biometric data interpretation.

***Keywords*---**Biometric devices, health management, pharmacists, data interpretation, patient guidance, electronic health records.

Introduction

In the contemporary digital landscape, the significance of secure and user-friendly authentication methods has reached a critical juncture due to the surge in online transactions, sensitive data management, and access to personal devices. Conventional authentication techniques, including passwords and PINs, are increasingly susceptible to cyber threats such as hacking, phishing, and identity theft. This vulnerability underscores the urgent need for more resilient and user-centric security solutions. Biometric security systems, which utilize distinctive physiological or behavioral attributes for user identification and verification, have emerged as a promising model for enhancing security, privacy, and user engagement across various applications. At the same time, the proliferation of wearable devices outfitted with biometric sensors has transformed how individuals engage with technology, facilitating the seamless incorporation of biometric authentication into daily routines and lifestyles. Biometric security systems signify a shift away from traditional knowledge-based authentication methods by depending on inherent and unchangeable biometric characteristics for identity verification. These biometric characteristics may encompass fingerprints, iris patterns, facial features, voiceprints, palm prints, and even

behavioral traits such as gait patterns and typing rhythms. By capturing and analyzing these unique biometric signatures, biometric security systems can authenticate individuals with a high degree of accuracy, thus reducing the risks linked to password-dependent authentication, including forgotten passwords, compromised credentials, and brute-force assaults.

The implementation of biometric security systems spans multiple sectors, including finance, healthcare, government, law enforcement, and consumer electronics, where secure and user-friendly authentication mechanisms are vital. In the banking and finance sectors, biometric authentication provides secure access to online banking platforms, mobile payment systems, and ATMs, thereby diminishing the risk of fraudulent transactions and unauthorized access to accounts. In healthcare, biometric identification safeguards the integrity of electronic health records (EHRs), protects patient privacy, and facilitates secure access to medical devices and pharmaceuticals. Government entities harness biometric technologies for purposes such as border control, immigration assessments, national ID programs, and law enforcement activities, thus enhancing public safety and national security. Biometric passports, driver's licenses, and voter registration systems incorporate biometric authentication to thwart identity fraud and ensure the accuracy and reliability of identity documents. Additionally, biometric surveillance systems facilitate the tracking and identification of individuals in public spaces, assisting in criminal investigations and counterterrorism initiatives. In the consumer electronics domain, biometric authentication has become increasingly common in smartphones, tablets, laptops, and wearable devices, providing convenient and secure access to personal devices and digital services. Integrated fingerprint sensors, facial recognition cameras, and iris scanners in smartphones enable rapid and dependable authentication, eliminating the need for cumbersome passwords and PINs. Wearable devices, such as smartwatches, fitness trackers, and biometric jewelry, are equipped with biometric sensors to monitor user health metrics, track physical activity, and offer personalized feedback and insights.
The intersection of biometric security systems and wearable devices signifies a paradigm shift in individual interactions with technology, merging the digital and physical realms. Wearable biometric sensors are seamlessly integrated into everyday accessories and clothing, facilitating continuous and unobtrusive monitoring of physiological and behavioral signals. This integration allows for context-aware authentication and personalized user experiences. By merging biometric authentication with wearable technology, users can securely access their devices, validate transactions, and engage with digital services without requiring explicit user input or manual intervention. Nonetheless, despite the myriad benefits and prospects presented by biometric security systems and wearable devices, several challenges and considerations persist. Issues related to privacy, data security, interoperability, standardization, and regulatory compliance are critical and must be addressed to ensure the responsible and ethical deployment of biometric technologies. Furthermore, concerns regarding the accuracy, reliability, and vulnerability to spoofing or presentation attacks, particularly in certain biometric modalities like facial recognition, highlight the need for robust security measures and ongoing innovation in biometric authentication algorithms and sensor technologies.

Fundamentals of Biometric Authentication

Biometric authentication constitutes an innovative method for verifying individual identities based on distinct biological characteristics. Among the most prevalent biometric identifiers are fingerprints, facial recognition, and iris scans. Fingerprint recognition relies on the unique patterns created by the ridges and valleys found on the fingertips. These patterns, commonly known as minutiae points, are captured using specialized sensors and subsequently compared against stored templates for the purpose of authentication. In contrast, facial recognition employs advanced algorithms to analyze facial features such as the distances between the eyes, nose, and mouth, generating a unique digital representation referred to as a facial template. Iris scanning captures high-resolution images of the iris—the colored part of the eye—and extracts its unique patterns for identification purposes. These biometric identifiers provide multiple advantages over traditional authentication methods such as passwords and PINs. One notable advantage of biometric authentication is its inherent convenience. Unlike passwords or PINs, which users are required to remember and often struggle to secure, biometric traits are intrinsic to individuals, eliminating the necessity for memorization. This convenience translates into time savings and an improved user experience, particularly in contexts requiring swift authentication, such as unlocking smartphones or entering secure facilities. Additionally, biometric authentication diminishes the likelihood of unauthorized access resulting from forgotten or stolen credentials, thereby enhancing security.

Furthermore, biometric identifiers provide a heightened level of security compared to traditional authentication methods. While passwords and PINs can be readily compromised through theft, interception, or brute-force attacks, biometric traits are uniquely associated with each individual and are considerably more challenging to replicate. This characteristic renders biometric authentication particularly effective in thwarting unauthorized access to sensitive information or restricted areas. Moreover, biometric systems can incorporate multi-factor authentication by integrating two or more biometric modalities (e.g., fingerprint and facial recognition), further strengthening security measures. Despite these benefits, biometric authentication also presents several challenges and considerations that necessitate attention. A primary concern pertains to privacy. Given that biometric data is inherently personal and immutable, its collection, storage, and usage raise significant privacy implications. There exists a risk of biometric information being misappropriated or exploited for surveillance purposes, thereby raising ethical and legal concerns. As such, robust privacy safeguards and regulatory frameworks are critical for ensuring the responsible management of biometric data and for protecting individual rights.

Another challenge involves the accuracy and reliability of biometric systems. Although biometric identifiers are unique to individuals, factors such as environmental conditions, variations in trait presentation, and limitations of sensors can influence the accuracy of biometric authentication. The false acceptance and false rejection rates—representing the erroneous acceptance of impostors and the wrongful rejection of legitimate users, respectively—are essential metrics for assessing biometric system performance. Striking a balance between security and usability necessitates the optimization of these rates to

minimize both false positives and false negatives. Additionally, biometric authentication systems are susceptible to spoofing attacks, where malicious actors attempt to bypass the authentication process by presenting counterfeit biometric traits. Tactics such as employing high-quality forged fingerprints or crafting realistic facial masks pose significant security challenges for biometric systems. To mitigate these risks, advanced anti-spoofing techniques, including liveness detection and biometric encryption, are utilized to distinguish between authentic biometric traits and fraudulent replicas.

Role of IoT in Biometric Authentication

The integration of the Internet of Things (IoT) into biometric authentication marks a notable advancement in both security and user experience by utilizing interconnected devices to capture and authenticate biometric information. IoT-enabled biometric authentication amalgamates biometric sensors and devices with IoT infrastructure, facilitating seamless and secure identity verification across diverse applications and environments. At its essence, IoT-enabled biometric authentication expands upon traditional biometric systems by integrating IoT devices equipped with biometric sensors. These sensors can capture a variety of biometric modalities, including fingerprints, facial features, and iris patterns. For instance, smart cameras may be installed in public areas or embedded within IoT-enabled devices to capture facial images for authentication purposes. Likewise, fingerprint scanners embedded in IoT devices such as smartphones or access control systems are capable of gathering fingerprint data for identity verification. The amalgamation of IoT devices with biometric sensors significantly enhances the flexibility and accessibility of biometric authentication. Users can conveniently authenticate their identities through familiar devices such as smartphones, tablets, or IoT-enabled wearables, thereby negating the need for specialized biometric hardware. This widespread accessibility to biometric authentication promotes its adoption across a variety of applications, including mobile banking, e-commerce, smart homes, and connected vehicles. Moreover, IoT-enabled biometric authentication utilizes cloud-based authentication platforms for the secure storage, processing, and verification of biometric data. Biometric templates gathered by IoT devices are encrypted and transmitted to cloud servers for authentication, facilitating centralized management and scalability. These cloud-based authentication platforms employ advanced algorithms and machine learning techniques to analyze biometric data and match it against stored templates, ensuring accurate and reliable identity verification.

The synergy between IoT and cloud technologies enhances the scalability and efficiency of biometric authentication systems, allowing for seamless integration with existing infrastructure and services. For example, IoT devices deployed within smart buildings or industrial environments can authenticate user identities for access control or time attendance purposes, utilizing cloud-based authentication platforms for centralized management and monitoring. In summary, the role of IoT in biometric authentication provides a transformative approach to identity verification, merging the capabilities of biometric sensors, IoT devices, and cloud-based authentication platforms to deliver secure, convenient, and scalable authentication solutions. By harnessing interconnected devices and cloud infrastructure, IoT-enabled biometric authentication paves the way for

innovative applications and services across multiple industries, fostering the evolution of digital identity management in the IoT era.

Components of IoT-Enabled Biometric Authentication Systems

IoT-enabled biometric authentication systems consist of several integral components that collaborate to capture, process, and authenticate biometric data in real time. These components include IoT sensors and devices, connectivity protocols, and edge computing capabilities.

IoT Sensors and Devices: Serving as the primary interfaces for capturing biometric data, IoT sensors and devices include biometric scanners such as fingerprint readers, facial recognition cameras, iris scanners, and voice recognition microphones. Additionally, IoT-enabled wearables, including smartwatches and fitness trackers, may incorporate biometric sensors to gather physiological data for authentication purposes. These devices are equipped with specialized hardware and software designed to accurately capture and process biometric traits.

Connectivity Protocols: Connectivity protocols facilitate communication between IoT devices and backend systems, enabling data transmission and authentication. Common protocols utilized in IoT-enabled biometric authentication systems include Wi-Fi, Bluetooth, and Near Field Communication (NFC). Wi-Fi connectivity permits IoT devices to transmit biometric data over local or wide-area networks, promoting seamless integration with cloud-based authentication platforms. Bluetooth supports short-range wireless communication between IoT devices and mobile devices or other peripherals, offering flexibility and convenience for authentication purposes. NFC technology allows for contactless communication between IoT devices and compatible smartphones or access control systems, making it ideal for applications such as mobile payments and access control.

Edge Computing and Processing: Edge computing involves processing and analyzing data at or near the source of data generation, such as within the IoT devices themselves. In IoT-enabled biometric authentication systems, edge computing capabilities are vital for performing real-time processing of biometric data, thus enabling rapid authentication. Edge computing devices, such as IoT gateways or edge servers, host specialized algorithms and machine learning models for tasks such as biometric feature extraction, template matching, and decision-making. By conducting processing tasks locally, edge computing reduces latency and bandwidth demands, thereby enhancing the responsiveness and reliability of biometric authentication systems. Furthermore, edge computing bolsters security by minimizing the transmission of sensitive biometric data over networks, reducing the risk of data interception or unauthorized access. In summary, the components of IoT-enabled biometric authentication systems encompass IoT sensors and devices for capturing biometric data, connectivity protocols for facilitating communication between devices and backend systems, and edge computing capabilities for real-time processing and analysis of biometric information. By integrating these components, IoT-enabled biometric

authentication systems provide secure, convenient, and efficient identity verification solutions across diverse applications and environments.

Security Considerations

Security considerations are critical in IoT-enabled biometric authentication systems to ensure the confidentiality, integrity, and availability of biometric data and authentication processes. Key security measures encompass encryption techniques for safeguarding biometric data during transit, authentication protocols for secure access control, and mitigation strategies to address security threats such as man-in-the-middle attacks and data breaches.

Encryption Techniques: These techniques play a pivotal role in securing biometric data during transmission between IoT devices and backend servers or cloud-based authentication platforms. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are commonly employed encryption protocols for securing Internet communications. TLS ensures data confidentiality and integrity by encrypting biometric data packets before transmission and decrypting them upon arrival at their intended destination. Additionally, the Advanced Encryption Standard (AES) encryption algorithms are frequently used to encrypt biometric templates stored on IoT devices or within cloud-based databases, thereby protecting them from unauthorized access or tampering.

Authentication Protocols: These protocols are essential for establishing secure access control mechanisms within IoT-enabled biometric authentication systems. OAuth (Open Authorization) and OpenID Connect are widely utilized authentication protocols that enable secure user authentication and authorization across distributed systems. OAuth allows users to delegate access control by granting permission to third-party applications to access their biometric data or authentication tokens without disclosing their credentials. OpenID Connect builds upon OAuth, providing a standardized framework for securely verifying user identities and exchanging authentication tokens between identity providers and relying parties. The implementation of robust authentication protocols ensures secure and seamless access control while safeguarding users' privacy and confidentiality.

Mitigation of Security Threats: Addressing security threats, such as man-in-the-middle attacks and data breaches, is crucial for protecting IoT-enabled biometric authentication systems from unauthorized access or manipulation of biometric data. Man-in-the-middle attacks involve intercepting and tampering with communications between IoT devices and backend servers, potentially compromising the confidentiality and integrity of biometric data. To mitigate this threat, secure communication protocols like TLS should be adopted to encrypt data transmissions, preventing eavesdropping or tampering by malicious actors. Furthermore, implementing mutual authentication mechanisms between IoT devices and backend servers can verify the authenticity of communication endpoints and prevent unauthorized access. Data breaches represent another significant security threat to IoT-enabled biometric authentication systems, as they can expose sensitive biometric data to unauthorized entities. To mitigate the risk of data breaches, comprehensive security measures—such as access control

policies, encryption, and data anonymization techniques—should be enforced to protect biometric data at rest and in transit. Conducting regular security audits and penetration testing can help identify vulnerabilities and weaknesses within the system architecture, enabling timely remediation and strengthening of security controls.

Examples of Biometrics in Health Management

Biometric technologies have increasingly been integrated into health management systems, enhancing the accuracy and efficiency of patient identification, monitoring, and treatment. Several notable applications include:

1. **Patient Identification and Verification**: Biometric systems, such as fingerprint and facial recognition technologies, are utilized to verify patient identities within healthcare facilities. This application reduces the likelihood of medical errors stemming from misidentification, ensuring that patients receive the correct treatment and medications.
2. **Access Control**: Biometric authentication mechanisms, including iris scanning and voice recognition, are employed to restrict access to sensitive areas within healthcare institutions, such as pharmacies and laboratories. By ensuring that only authorized personnel can access restricted areas, these systems enhance the security of medical records and pharmaceuticals.
3. **Remote Patient Monitoring**: Wearable biometric devices, such as smartwatches and fitness trackers, enable healthcare providers to remotely monitor patients' vital signs and other physiological parameters. For instance, continuous heart rate monitoring through biometric sensors facilitates the early detection of potential health issues, allowing for timely interventions.
4. **Chronic Disease Management**: Biometric technologies are instrumental in managing chronic diseases, such as diabetes and hypertension. For example, biometric-enabled glucose monitors can automatically transmit glucose levels to healthcare providers, allowing for real-time adjustments in treatment plans.
5. **Telehealth Services**: The integration of biometrics in telehealth platforms enhances patient authentication and security. Biometric verification can be utilized to confirm the identity of patients during virtual consultations, ensuring that sensitive health information remains secure.

The Role of Pharmacists

Pharmacists play a crucial role in the integration of biometrics into health management, contributing to various facets of patient care and medication management:

1. **Medication Safety**: Pharmacists can leverage biometric technologies to verify patient identities during medication dispensing. This practice minimizes the risk of medication errors by ensuring that patients receive the correct prescriptions based on their unique biometric identifiers.
2. **Patient Counseling**: With access to biometric data, pharmacists can provide tailored counseling and education to patients regarding their health conditions and medications. For instance, understanding a

patient's biometric data, such as blood pressure readings, enables pharmacists to offer personalized advice on lifestyle modifications and adherence to treatment regimens.

3. **Chronic Disease Management**: Pharmacists can utilize biometric monitoring data to assist in the management of chronic diseases. By analyzing biometric trends, pharmacists can collaborate with healthcare teams to optimize medication therapy and improve patient outcomes.
4. **Data Security and Privacy**: Pharmacists are responsible for ensuring the confidentiality and integrity of biometric data collected during patient interactions. By adhering to stringent data protection protocols, pharmacists can maintain the trust of patients in the use of biometric technologies.
5. **Integration of Technology in Practice**: As healthcare increasingly incorporates biometric technologies, pharmacists are positioned to lead the integration of these systems within pharmacy practice. This includes advocating for the adoption of biometric solutions in medication management and ensuring their effective implementation.

In conclusion, the application of biometrics in health management offers significant benefits, including enhanced patient identification, improved medication safety, and effective chronic disease management. Pharmacists, as vital members of the healthcare team, play an essential role in harnessing the potential of biometric technologies to improve patient care and outcomes. By integrating biometrics into their practice, pharmacists contribute to the advancement of health management systems and the overall enhancement of healthcare delivery.

Conclusion

The integration of biometric devices in health management presents a transformative shift in the delivery of healthcare services. These technologies, which leverage unique physiological and behavioral traits for patient identification and data security, offer unprecedented advantages in ensuring accurate patient records, safeguarding sensitive health information, and streamlining healthcare processes. Pharmacists, as accessible healthcare professionals, are uniquely positioned to play a pivotal role in this evolving landscape. Their responsibilities extend beyond traditional pharmaceutical care to include the interpretation of biometric data, which is essential for enhancing patient outcomes. Pharmacists' involvement in biometric data interpretation ensures that patients receive comprehensive guidance on the implications of biometric technologies. They can assist patients in understanding how these devices function, the significance of the data collected, and how to integrate biometric feedback into their healthcare management strategies. This patient-centered approach not only fosters better adherence to medication regimens but also empowers individuals to take an active role in managing their health. Moreover, pharmacists can leverage biometric devices to monitor chronic conditions such as diabetes and hypertension. Continuous monitoring through biometric sensors allows for timely interventions and adjustments in therapy, contributing to improved patient outcomes. In addition, pharmacists can collaborate with other healthcare professionals to establish protocols that integrate biometric data into clinical

decision-making processes, thereby enhancing the overall quality of care. Despite the promising potential of biometric technologies, several challenges must be addressed. These include concerns related to data privacy, the accuracy of biometric measurements, and the need for regulatory frameworks to guide their implementation in healthcare settings. As these challenges are navigated, the role of pharmacists in guiding patients through the complexities of biometric data will become increasingly critical. In conclusion, the incorporation of biometric devices in health management represents a significant advancement in healthcare delivery. Pharmacists, with their expertise and accessibility, are essential in interpreting biometric data and guiding patients towards effective health management. This partnership between technology and pharmacy practice not only enhances the patient experience but also paves the way for more personalized and efficient healthcare solutions. Future efforts should focus on expanding the role of pharmacists in this domain through targeted training and the development of best practices for the utilization of biometric data in health management.

References

1. Coelho, K. K., Tristão, E. T., Nogueira, M., Vieira, A. B., & Nacif, J. A. (2023). Multimodal biometric authentication method by federated learning. *Biomedical Signal Processing and Control*, *85*, 105022.
2. Ahmed, I., & Asghar, A. (2023). Evaluating the Efficacy of Biometric Authentication Techniques in Healthcare. *International Journal of Responsible Artificial Intelligence*, *13*(7), 1-12.
3. Pereira, T. M., Conceição, R. C., Sencadas, V., & Sebastião, R. (2023). Biometric recognition: A systematic review on electrocardiogram data acquisition methods. *Sensors*, *23*(3), 1507.
4. Goergen, C. J., Tweardy, M. J., Steinhubl, S. R., Wegerich, S. W., Singh, K., Mieloszyk, R. J., & Dunn, J. (2022). Detection and monitoring of viral infections via wearable devices and biometric data. *Annual review of biomedical engineering*, *24*(1), 1-27.
5. Ahamed, F., Farid, F., Suleiman, B., Jan, Z., Wahsheh, L. A., & Shahrestani, S. (2022). An intelligent multimodal biometric authentication model for personalised healthcare services. *Future Internet*, *14*(8), 222.

الأجهزة البيومترية في إدارة الصحة: مساهمة الصيادلة في تفسير البيانات وإرشاد المرضى

الملخص:

الخلفية :إن التقدم السريع في تكنولوجيا الأجهزة البيومترية في إدارة الصحة قد فتح آفاقًا جديدة لتحديد هوية المرضى وضمان أمان البيانات. مع اعتماد أنظمة الرعاية الصحية بشكل متزايد على الأجهزة البيومترية، هناك حاجة متزايدة لمتخصصي الرعاية الصحية، ولا سيما الصيادلة، لتفسير البيانات البيومترية بشكل فعال.

الهدف :يهدف هذه الدراسة إلى استكشاف دور الصيادلة في استخدام الأجهزة البيومترية في إدارة الصحة، مع التركيز على مساهمتهم في تفسير البيانات وإرشاد المرضى.

الطرق :تم إجراء مراجعة شاملة للأدبيات، حيث تم تحليل دراسات متنوعة حول الأجهزة البيومترية في الرعاية الصحية ومشاركة الصيادلة. تركز البحث على أنواع تقنيات البيومترية المستخدمة، ومسؤوليات الصيادلة، ودراسات الحالة التي تسلط الضوء على التطبيقات الناجحة.

النتائج :تكشف النتائج أن الصيادلة يلعبون دورًا حاسمًا في تفسير البيانات البيومترية، وتعليم المرضى عن آثارها، وضمان الالتزام بخطط العلاج الدوائي. كما يساعدون في إدارة الأمراض المزمنة من خلال المراقبة المستمرة التي تتيحها الأجهزة البيومترية. علاوة على ذلك، يسهل الصيادلة مشاركة المرضى من خلال تعزيز فهمهم وقبولهم لتقنيات البيومترية.

الخاتمة :مع تحول الأجهزة البيومترية إلى جزء لا يتجزأ من إدارة الصحة، فإن الصيادلة في وضع جيد لقيادة تفسير البيانات وتعليم المرضى. تعزز مشاركتهم سلامة المرضى، وتحسن النتائج العلاجية، وتؤدي إلى نهج أكثر شمولية في تقديم الرعاية الصحية. يجب أن تركز الأبحاث المستقبلية على تطوير بروتوكولات موحدة لتدريب الصيادلة في تفسير البيانات البيومترية.

الكلمات المفتاحية :الأجهزة البيومترية، إدارة الصحة، الصيادلة، تفسير البيانات، إرشاد المرضى، السجلات الصحية الإلكترونية.