International Journal of Social Science and Public Policy

VOL: 6, ISSUE: 6
June/2024
https://ijssppnet.com/
E-ISSN: 2663-7200
http://dx.doi.org/10.33642/ijsspp.v6n6p1

Survey of Information Security and Privacy for Patient-Generated Health Data

James Burrell, Ph.D.
Boston College, USA
Email: james.burrell@bc.edu
USA

ABSTRACT

Mobile health technologies enable self-monitoring of health and fitness conditions for personal health and lifestyle management with the potential to improve the quality, accuracy, and cost of healthcare. The advancement of connected and precision healthcare services requires a variety of health information which includes patient-generated health data. The collection, processing, and management of personal health information with mHealth devices and sensors represent unique and substantial risks to the security and privacy of personal health data. Current laws, regulations, and policies have primarily addressed the privacy of patient health information collected and maintained by healthcare and clinical providers but have not fundamentally addressed patient-generated health data. This paper provides an overview of information security, assurance, and data governance principles of connected healthcare with a focus on patient-generated health data and informs the development of policies, standards, and guidelines for sensitive health information.

KEYWORDS: Mobile health, health data, security, privacy, public policy

Introduction

A research study conducted by International Data Corporation (IDC) determined that an expected 1.2 billion smartphones will be shipped in 2024, a 2.8% increase from the previous year, with an expectation to reach 1.3 billion in 2028 (Scarsella, 2024). An additional study determined that wearable device shipments for 2024 were expected to reach 559.7 million, a 10.5% increase over 2023, with an expectation to reach 645.7 million in 2028 (Ubrani et al., 2024). There has also been an increase in 5G wireless data accessibility and cloud-based integrations which enable real-time data transfer from IoT, IoMT, and other mHealth devices.

In terms of the adoption rate for these mHealth devices and applications, a recent survey in 2023 determined an increase in the use of health applications and wearable devices with 40% of adults using health-related applications and 35% using wearable health devices (Vaidya, 2023). The global wearable medical device market is projected to increase from $73.77 billion in 2023 to $428.92 billion in 2030 as illustrated in Figure 1 (Fortune Business Insights, 2024).

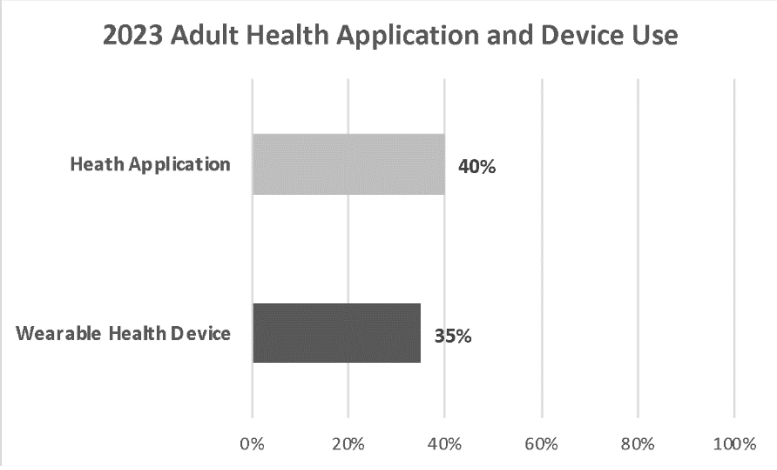

Figure 1. 2023 Adult Health Application and Device Use.

Note. Data from "Over a Third of Adults Use Health Apps, Wearables in 2023, Up from 2018," by A. Vaidya, Copyright 2012-2024 TechTarget, Inc. and "Wearable Medical Devices Market Size Research Report [2030]," by Fortune Business Insights, Copyright 2024 by Fortune Business Insights.

The evolution of digital health technology has enabled the integration of medical devices, wireless communications, data storage systems, and wearable devices and sensors to provide real-time health, fitness, and activity data acquisition (Kelly et al., 2022). These advancements include the adoption of digital mobile health (mHealth) systems that enable options for telehealth, remote patient monitoring, treatment, and self-managed healthcare (Kumar, 2023). These devices and sensors include small-scale computers categorized as Internet of Things (IoT), Healthcare Internet of Things (H-IoT), and Internet of Medical Things (IoMT) that enable noninvasive and continuous monitoring of vital physiological parameters, remote patient monitoring, and patient managed healthcare (Babu et al., 2024). These wireless interconnected health and fitness sensors may include activity, weight, temperature, continuous glucose, blood pressure, heart rate, pulse oximeter, electrocardiogram,

International Journal of Social Science and Public Policy

VOL: 6, ISSUE: 6
June/2024
https://ijssppnet.com/
E-ISSN: 2663-7200
http://dx.doi.org/10.33642/ijsspp.v6n6p1

and other devices. The volume and diversity of the data generated by these devices could improve individual and population health prevention, treatment, and cost of care. Portability, scalability, and affordability are key differentiators for these small-scale devices to generate continuous health and fitness information that is ordinarily unavailable or inaccessible by clinical healthcare systems or providers.

Personal health information (PHI) located on these devices or technologies provides essential details to facilitate the diagnosis and treatment of patient medical conditions that are increasingly being utilized to support clinical, research, and administrative requirements for hospitals, private practitioners, and insurance companies. The health data maintained by institutional health information management systems are essential to maintain high levels of quality, accuracy, efficiency, and reduced cost of healthcare. The digital transformation in the healthcare sector continues to provide technology-enhanced health services with insights that are based partially on the evaluation of electronic patient health information (ePHI) in electronic health records (EHR) and other health information systems and medical monitoring devices.

Network-enabled mHealth devices and sensors transfer health and fitness data to a smartphone or remote system using Bluetooth, Wi-Fi, or other wireless communications protocols. The data may also be transferred to a cloud-based storage system managed by the manufacturer or third-party entity that provides users with the ability to organize, process, and visualize PGHD device data (Babu et al., 2024). The transfer of PGHD to third-party service providers that are not affiliated with clinical providers or healthcare organizations introduces varying levels of patient health data security and privacy risk considerations. The security and privacy of PGHD require the use of secure encryption algorithms, software design, endpoint monitoring, and remote data deletion (Abouelmehdi et al., 2017).

The integration of mHealth data with other systems also introduces security, privacy, and safety risks that require careful consideration. The data processing segments for mHealth devices including acquisition, storage, processing, and transmission are detailed in Figure 2.

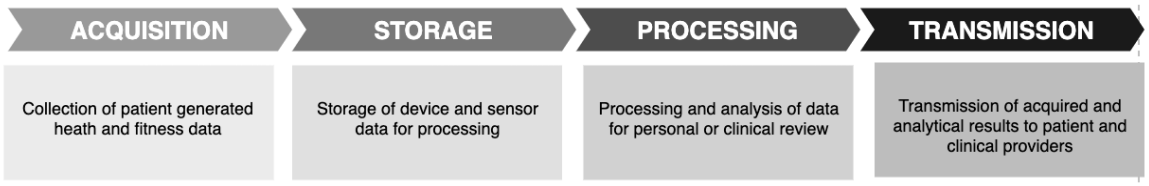

Figure 2. mHealth Device Data Processing Segments

The data acquisition and storage segments are performed by mHealth devices and applications with data storage, processing, and transfer functions increasingly being performed in cloud-based environments managed by the device manufacturer or application developer. It is recognized that the integration of patient-generated health and fitness data with clinical providers and healthcare institutions has defined benefits for personal health and fitness monitoring and sharing, but the security and privacy risks models change where the access, use, and dissemination of this data is determined by applicable terms and conditions, privacy policies, and practices defined by product manufacturer and service providers.

Health Information and Patient-Generated Health Data

An increasing number of privacy laws and regulations are being enacted in different national and international jurisdictions for the collection, processing, storage, and use of personal data. Before delving into these, the terms health information and patient-generated health data (PGHD) need to be defined. Health information pertains to a broad set of data related to current or previous medical or mental health conditions, diagnoses, and treatments. There are specific regulatory and legal terms that describe the subset of information related to Protected Health Information (PHI)/electronic Protected Health Information (ePHI). These regulations have typically applied to electronic health records (EHR) collected and maintained by covered healthcare entities and business associates. Patient-generated health data, on the other hand, includes information created or produced by consumer mHealth devices and applications as opposed to commercial medical diagnostic equipment utilized by healthcare institutions or clinical providers. The definition of patient-generated health data from the U.S. Office of the National Coordinator for Health Information Technology (ONC) is "Patient-generated health data (PGHD) are health-related data created, recorded, or gathered by or from patients (or family members or other caregivers) to help address a health concern" (U.S. Office of the National Coordinator for Health Information Technology, 2017).

The acquisition, storage, and management of health information represents an increasingly complex environment for security, privacy, and governance (Transform Health, 2022). Health Data Governance Principles were introduced by Transform Health in 2022, primarily based on an inclusive and consultative process that involved 200 contributors, 130 organizations, and five regional and three global workshops to extend current principles, treaties, and guidelines. These principles included recommendations presented as Protect People, Promote Health Value, and Prioritize Equality which recognize the importance of Build Trust in Data Systems, Ensure Data Security, Promote Data Sharing and Interoperability, and Establish Data Rights and Ownership (Transform Health, 2022).

The primary U.S. regulation for health data governance is the Health Insurance Portability and Accountability Act (HIPAA) established in 1996 which includes protections for healthcare information privacy. This regulation addresses safeguards for physical and electronic records for both PHI and e-PHI whereas the HIPAA Security Rule applies to any healthcare provider that

International Journal of Social Science and Public Policy

VOL: 6, ISSUE: 6
June/2024
https://ijssppnet.com/
E-ISSN: 2663-7200
http://dx.doi.org/10.33642/ijsspp.v6n6p1

transmits health information in an electronic format (Kelly et al., 2022). The HIPAA Security Rule has specific references for the assurance of confidentiality, integrity, and availability of e-PHI for any healthcare provider including administrative procedures, physical controls, and technical controls. The HHS Summary of the HIPAA Security Rule provides definitions for these terms about electronic ePHI information summarized in Table 1 (U.S. Centers for Disease Control and Prevention, 2024).

Principle	Information Security Compliance Measure
Confidentiality	ePHI is not disclosed to an unauthorized entity
Integrity	ePHI is not altered or destroyed in an unauthorized manner
Availability	ePHI is accessible and usable on demand by an authorized entity

Table 1. Summary of the HIPAA Security Rule terminology

The U.S. Department of Health and Human Services (HHS) Standards for Privacy of Individually Identifiable Health Information provides comprehensive legal protections for health information privacy and the HIPAA Privacy Rule including specific protections for individually identifiable health information (U.S. Department of Health and Human Services, 2008). The HIPAA Privacy, Security, and Breach Notification Rules collectively establish comprehensive legal protections for individually identifiable health information or PHI when created, received, maintained, or transmitted by a HIPAA-covered entity or business associate, including limitations on uses and disclosures of such information, safeguards against inappropriate uses and disclosures, and individuals' rights concerning their health information (U.S. Department of Health and Human Services, 2008).

Despite the security and privacy provisions of HIPAA, other entities could potentially be considered to be covered by health information security and privacy regulations and policies in addition to those specified below (U.S. Centers for Disease Control and Prevention, 2024):

- Healthcare providers
- Healthcare clearinghouses
- Health plans
- Business associates

A key consideration is the HIPAA and GDPR do not specify or mandate specific processes or controls for the assurance of confidentiality or integrity of personal or health data but require the implementation of appropriate measures to satisfy regulatory requirements. The developers of eHealth devices, applications, and services are not generally considered to be covered entities by HIPAA except in instances when PGHD is requested or provided to a covered entity where the information would be subject to applicable HIPAA security and privacy provisions (HealthITSecurity, 2018).

In contrast, there are international regulatory frameworks including the European Union (EU) General Data Protection Regulation (GDPR) enacted in 2018 that apply generally to personal information with specific references to assurance of confidentiality and integrity of personal data. This privacy law provides fundamental protection for personal health data that governs the data within and transferred externally from the EU and European Economic Area (EEA) (Kelly et al., 2022).

One-way confidentiality was addressed in the U.S. is with the finalization of the U.S. Federal Trade Commission's (FTC) Health Breach Notification Rule in April 2024 that addresses mHealth applications and other health information technologies not currently covered by HIPAA (U.S. Federal Trade Commission, 2009; U.S. Federal Trade Commission, 2024). The Health Breach Notification Rule requires foreign and domestic entities and third-party service providers that maintain personal health records (PHR) of U.S. citizens or residents (U.S. Federal Trade Commission, 2009). The rule defines PHR as an electronic record of individual identifiable health information that is managed, shared, and controlled by or primarily for the individual, and the term unsecured PHR as identifiable information that is not protected using technology or methodology (U.S. Federal Trade Commission, 2009). However, this addresses confidentiality after the fact versus having a proactive preventative strategy.

Consumer Health Data and Privacy Policies

mHealth devices and sensors can continuously monitor patient health and fitness activities to achieve optimized health and provide unique insight into the diagnosis, treatment, and management of medical conditions. The collection of PHI represents a potential risk to personal privacy and relies on the transparency of the manufacturer or entity that collects or manages PHI data. Consumers need to understand that PGHD collected, processed, and stored by mHealth devices is not necessarily subject to the privacy protections provided by HIPAA, GDPR, or other laws or regulations.

Manufacturers of mHealth devices, applications, and data management services may have separate privacy and consumer health data privacy policies. A privacy policy explains how an organization collects, processes, stores, protects, and shares customer information that may include personal, transactional, Internet Protocol address, geolocation, device, and other customer-related data for improved customer experience, marketing, and other purposes that include sharing with third-party entities. A consumer health data privacy policy specifically addresses health, medical, psychological, treatment, prescription, and other sensitive health information. An example of the categories of data included in these policies is provided below (Abbott Laboratories, 2024):

- Health condition
- Medication
- Diagnosis or diagnostic testing
- Prescriptions
- Disease or diagnosis
- Bodily function
- Treatment
- Vital sign
- Social, psychological, behavioral
- Symptoms
- Medical intervention information
- Measurement of physical or mental health status
- Health-related surgery or procedure
- Reproductive health

A comparison of consumer health data privacy policies for manufacturers of leading digital blood pressure monitors and continuous blood glucose monitors had similar definitions for

International Journal of Social Science and Public Policy

VOL: 6, ISSUE: 6
June/2024
https://ijssppnet.com/
E-ISSN: 2663-7200
http://dx.doi.org/10.33642/ijsspp.v6n6p1

consumer health data which can be summarized as personal information that is linked or can be reasonably linked to the past, present, or future physical or mental health status (Abbot Laboratories, 2024; OMRON Healthcare,2024). These consumer health data privacy policies provide clarification of current organizational practices that include health data is not sold or shared with third parties or associates with recognition that these terms may be updated by the device manufacturers with notification to consumers.

Health Information Security and Assurance Risk

Healthcare information technology and management systems store, process, and exchange a large amount of sensitive patient and diagnostic information accessible by electronic medical record (EMR) systems. mHealth devices are increasingly contributing to data accessible to EMR systems. The centralization of medical records presents advantages related to accessibility while this also introduces the risk and impact of a compromise of the confidentiality, integrity, and availability of EMR systems. Health information security and assurance is a critical function to enhance and protect the security and privacy of sensitive personal health information. Heath data governance, data protection laws, and privacy regulations are intended to specifically protect individuals, groups, and communities from harm and potential misuse (Transform Health, 2022).

The increase in the number of health information data breaches illustrates the magnitude of the risk to sensitive health data. A report released by Fortified Health Security concluded that the number of data breaches containing PHI doubled between 2022 and 2023, where the U.S. Health and Human Services (HHS) Office of Civil Rights (OCR) received 720 reports of data breaches that involved 500 records or more equated to over 133 million records that were "exposed" or "impermissibly disclosed" which is illustrated in Figure 3 (Olsen, 2024; Murray-Watson, 2024).

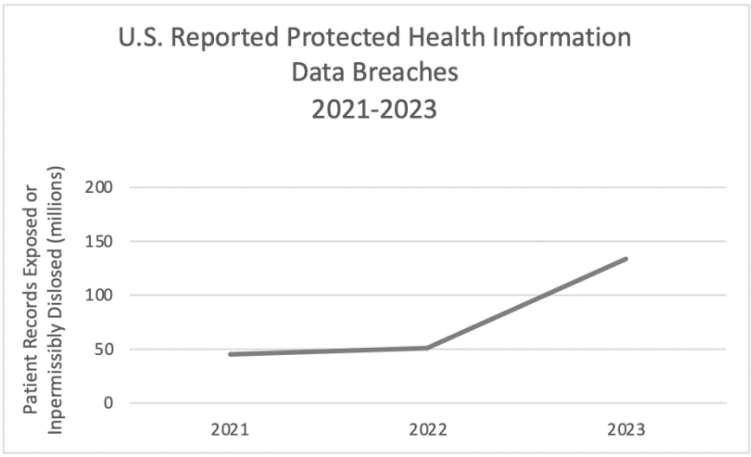

Figure 3. U.S. Reported Health Information Data Breaches 2021-2023.

Note. Data from "Healthcare Data Breach Statistics," by R. Murray-Watson, Copyright 2014-2024 by The HIPAA Journal.

There are no widely available statistics related to unauthorized data leaks or disclosures of PGHD based partially on the absence of regulatory notification requirements for eHealth devices and applications. The compromise or unauthorized access to PGHD, even if reported, could include a variety of other non-health data. In addition, mHealth sensors, devices, applications, and data could exist external to the enterprise information technology environment of healthcare organizations or other regulatory-covered entities.

Current Challenges for mHealth Devices and PGHD

The scalable adoption and integration of mHealth devices and data introduce several unique challenges. A series of selected challenges that impact mHealth devices and PGHD are detailed in Figure 4.

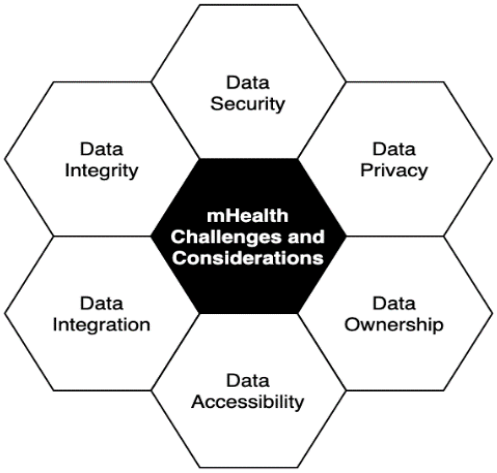

Figure 4. Selected mHealth Challenges and Considerations

International Journal of Social Science and Public Policy

VOL: 6, ISSUE: 6
June/2024
https://ijssppnet.com/
E-ISSN: 2663-7200
http://dx.doi.org/10.33642/ijsspp.v6n6p1

A description of these challenges for mHealth and PGHD are described in additional detail in the following section:

Data Security and Privacy

Confidentiality provides a level of assurance that access and disclosure of information is restricted to authorized entities. The complexity of the resource constraints of mHealth and embedded IoT, H-IoT, and IoMT devices. A study on Wearable Devices: Implications for Precision Medicine and the Future of Health Care estimated that wearable devices can generate over one terabyte (1 TB) of data during one year (Babu et al., 2024). The volume of PGHD also raises a potential concern for the security, privacy, use, and disclosure of personal health and fitness information acquired by these devices, sensors, and cloud storage platforms. The implementation of supplemental compensatory controls is often required to achieve equivalent privacy, security, and safety of PGHD. A combined assessment of patient health data security and privacy risk considerations is illustrated in Figure 5.

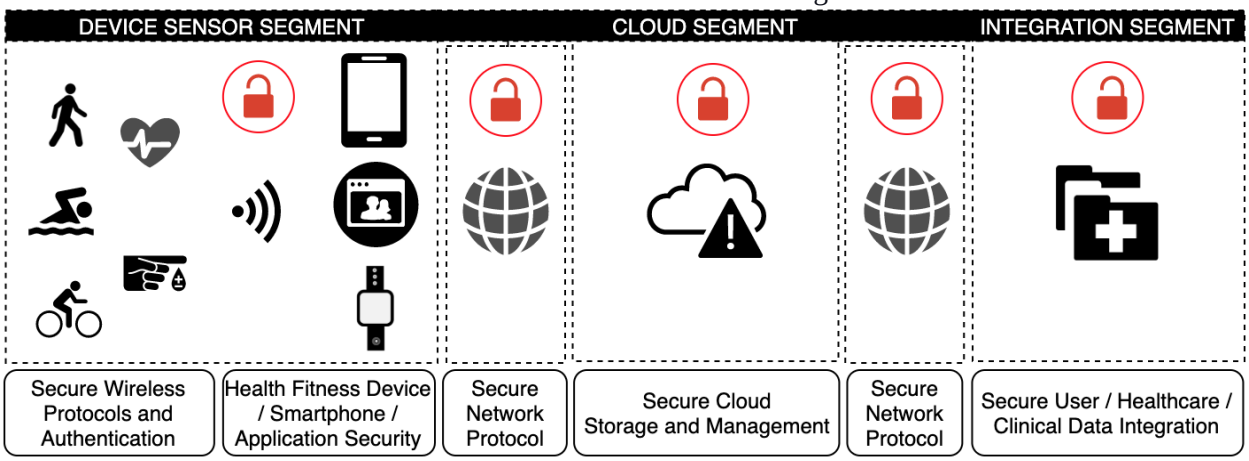

Figure 5. Electronic Patient Health Data Security and Privacy Risk Considerations.

The threats, vulnerabilities, and risks combined with mobile and wearable computing devices require the identification and implementation of appropriate security controls. The configuration and vulnerabilities associated with software applications represent a considerable risk to the security, integrity, privacy, and availability of PGHD. In addition, the volume and diversity of formats associated with mHealth devices and sensor data create additional complexities for cloud-based storage and analytical platforms.

Data Anonymization

Data anonymization is important to maintain user privacy for information disclosure or research. This privacy-enhancing method could include tokenization and other techniques for the removal of individual identifiers to reduce the risks associated with privacy requirements.

Physical Security

Wearable mHealth devices are constantly attached to the user but depending on the specific applications other devices may be unattended and physically accessible which presents an opportunity for unauthorized access, compromise, or theft of a device that contains PGHD. Device configuration and accessible security options should be enabled to protect or reduce physical attacks or compromise.

Data Encryption

mHealth devices may have limited processing, memory, and power capacity due to their small-scale design to support advanced encryption standards and algorithms. The hardware and software vulnerabilities impacting mHealth devices could result in increased susceptibility to compromise. The research and development of lightweight encryption algorithms provide resource-constrained small-scale computing devices with options to provide an enhanced level of security for the storage, processing, and transmission of PGHD. A recent research study involved the development of a proposed Lightweight medical-image encryption technique for IoMT-based healthcare applications that utilized a substitution permutation network technique to provide data security that was also shown to be resilient to selected attack methods (Islam et al., 2024).

Authentication

Authentication methods are utilized to validate user identity and prevent unauthorized access to systems and data. In addition, there is an associated concept of non-repudiation that provides the ability to positively identify the activities of an authorized user. A recent research study involved a survey of Authentication protocols for securing IoMT that included blockchain, artificial intelligence, biometrics, and other technologies for use in the IoMT environment (Singh & Garg, 2024).

Data Integrity

The assurance that PGHD is complete, accurate, and auditable is a critical requirement for the analysis of health data. The importance of these characteristics increases as PGHD is being integrated with EHRs for clinical diagnosis, treatment, and decision support (Ye et al., 2024). The potential benefits of Blockchain and other decentralized ledger system technology include enhancements for secure, transparent, and resilient protection of transaction data to provide verifiable, auditable, and tamper-resistant medical records (Corte-Real, 2024).

Data Integration and Interoperability

The integration of electronic PGHD integration with an EHR system allows clinical providers to combine the data with existing information contained in the patient record to visualize and detect trends, anomalies, and conditions to provide opportunities for the improvement of patient care (U.S. Department of Health and Human Services, 2021).

International Journal of Social Science and Public Policy

VOL: 6, ISSUE: 6
June/2024
https://ijssppnet.com/
E-ISSN: 2663-7200
http://dx.doi.org/10.33642/ijsspp.v6n6p1

The PGHD integration process requires information technology coordination between the mHealth device or application developer, the EMR developer, and the healthcare institution or provider. A primary integration issue relates to data standardization, quality, and any applicable legal, regulation, or policy restrictions or requirements that would be impacted by the convergence or dissemination of PGHD.

As an example, Apple has established EMR integration requirements that require end-to-end encryption of customer health and fitness data (Apple Inc., 2024).

In addition to information technology requirements, the referenced U.S. Department of Health and Human Services Agency of Healthcare Research and Quality identified several considerations for PGHD integration that included organizational readiness, data governance, privacy and security, and legal, compliance, security frameworks, and common data formats. There are common data format specifications that include the Fast Healthcare Interoperability Resources (FHIR) standard but there is no assurance that any of the standards have been adopted by the mHealth device manufacturer. Some vendors offer technical and compliance expertise for integration, interoperability services, and health data sharing (Craft, 2024).

Data Availability and Accessibility

The availability of PGHD data is essential to the continuous monitoring of health conditions. Several conditions could result in the lack of availability of data from device malfunction, power interruption, wireless interference, and connectivity to network services. In certain conditions, the recoverability of the data is limited to the internal memory capacity of the mHealth device or sensor which could result in partial or complete loss of PGHD. A software vulnerability or targeted attack that involves denial of service of system or wireless connectivity is another consideration that could be the result of intentional or unintentional factors.

The combination of these challenges and considerations demonstrates the complexities of providing a secure operating environment for eHealth devices and the management of PGHD. The association between selected health data governance and information security principles with corresponding security controls and configuration settings is detailed in Table 2.

Health Data Governance Principle	Information Security and Assurance Principle	Type	Security Control	Default Setting
Data Security	Confidentiality	Data at Rest	Encryption	Enabled
Protect Individuals and Communities	Confidentiality	Data in Transit	Encryption	Enabled
Build Trust in Data Systems	Integrity	Data Integrity	Encryption	Enabled
Access	Accessibility	Data Sharing	Authentication	Disabled

Table 2. Association of mHealth Data Governance and Information Security Principles

The Apple iOS platform is an example of a mHealth implementation that provides security, and privacy for PGHD. Their integrated health and fitness sensors, iHealth application, and iCloud storage platform provide comprehensive data security and privacy features which are summarized in Table 3 (Apple Inc., 2024).

Data Segment	Data Element	Default Setting	Type
Device	Data at Rest	Enabled	Encryption
Communications	Data in Transit	Enabled	Encryption
Cloud	Data at Rest	Enabled	Encryption
Access	Data Sharing	Disabled	Authorization

Table 3. Summary of Apple iOS Security and Privacy Features

Apple has adopted a comprehensive standard-based approach to security and privacy that includes the internationally recognized Factor Analysis of Information Risk (FAIR) quantitative model for risk-based cybersecurity and operational management compliance (Apple Inc., 2024; Fair Institute, 2024). Other devices and technology integrations provide partial or similar security and privacy.

Governance and Policy Considerations

The advancement of mHealth and PGHD continue to enable a healthier lifestyle and self-managed healthcare and provide healthcare institutions with critical data to improve monitoring, diagnosis, and treatment. The sensitivity of ePHI is globally recognized with the enactment of security and privacy laws, regulations, and policies to protect sensitive health information. The effectiveness of governance measures is constantly challenged by the transformative changes in technology and access to sensitive health data.

The evaluation of risks associated with the integration of PGHD requires careful analysis to determine the extent of the impact and potential mitigation options. Selected evaluative policy and governance recommendations that correspond to health data principles associated with mHealth and PGHD are presented in Table 4.

Health Data Principles	Policy and Governance Considerations
Legislation and Regulation	• Align legislative and regulatory requirements for PHI, ePHI, and PGHD. • Standardization of consumer health data privacy policies that provide full transparency with a privacy impact analysis for the data use, sharing, identification and reidentification of health and PGHD.
Security and Privacy	• Assessment and alignment of national laws and regulations to recognize PGHD as sensitive health data. • Identify of legal, regulatory, and policy definitions, descriptions, and

International Journal of Social Science and Public Policy

VOL: 6, ISSUE: 6
June/2024
https://ijssppnet.com/
E-ISSN: 2663-7200
http://dx.doi.org/10.33642/ijsspp.v6n6p1

	requirements that will effectively maintain pace with technological change. • Promote security and privacy by design as the guiding principles for the development and reduction of vulnerabilities and risk to mHealth devices, sensors, applications, and data. • Increase consumer awareness of the security and privacy risks associated with the collection, storage, and sharing of PGHD. • Support research for the development of usable security solutions and technologies for small-scale computing devices, sensors, and applications that collect, store, and process PGHD. • Establish quality, accuracy, and safety standards and measures in coordination with regulatory agencies for mHealth devices and PGHD that promotes confidence for clinical and research use and opportunities.
Data Integrity	• Support research for the development of usable security solutions and technologies for small-scale computing devices, sensors, and applications that collect, store, and process PGHD. • Research and development of authentication algorithms and biometric technologies to promote authorized access and transfer of PGHD. • Evaluate the benefits and risks associated with the integration of Blockchain and other distributed technologies to provide trusted and auditable transactions of PGHD.
Data Integration	• Expand current approaches to a common data standards and health data taxonomy to include categories for PGHD. • Development of enhanced data integration processes for EMR systems to allow for the inclusion of extended categories of PGHD for healthcare and clinical providers. • Expand hardware and software development frameworks for mHealth devices and applications that include PGHD elements for large scale data storage and analysis.
Data Ownership	• Consider implementation of data minimization models for collection, processing, and storage of PGHD on mHealth devices, sensors, and cloud storage systems. • Evaluate the benefits and risks associated with the integration of artificial intelligence and other emerging technologies. • Increase consumer control for the sharing of PGHD and associated data that allows the inclusion or exclusion of specific categories to preserve personal privacy. • Increased transparency and default consumer opt out for monetization or other benefit provided to mHealth device manufacturers, application developers, storage services, or other third party from the integration of PGHD with other data that creates privacy increased risk to the consumer.
Availability and Accessibility	• Increase awareness for the benefits and use of mHealth devices and data. • Prioritize the development of solutions that promote equal access and use of mHealth devices and PGHD data to improve health.

Table 4. Mobile Health (mHealth) and Patient-Generated Health Data (PGHD)Governance and Policy Considerations.

The specific elements evaluated during the creation or change in policy and governance depend on several complex factors, and the listed recommendations represent potential topical considerations related to health data principles.

Conclusion

The opportunities and challenges for mHealth and PGHD continue to evolve and require continuous assessment to evaluate potential risks to security, privacy, integrity, integration, data ownership, and availability. The U.S. healthcare industry and medical device manufacturers have attempted to maintain pace with innovation, digital transformation, and potential impact on personal health information. However, opportunities exist for the government, healthcare institutions, and mHealth device and application developers to enable connected health innovation while identifying options to reduce potential risks to security, privacy, and confidentiality.

References

Abbott Laboratories. (2024, March 31). Consumer Health Data Privacy Policy | Abbott U.S. https://www.abbott.com/privacy-policy/consumer-health-data.html

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. Procedia Computer Science, 113, 73–80. https://doi.org/10.1016/j.procs.2017.08.292

International Journal of Social Science and Public Policy

VOL: 6, ISSUE: 6
June/2024
https://ijssppnet.com/
E-ISSN: 2663-7200
http://dx.doi.org/10.33642/ijsspp.v6n6p1

Apple Inc. (2023, September 8). Legal—Health App & Privacy—Apple. Apple Legal. https://www.apple.com/legal/privacy/data/en/health-app/

Apple Inc. (2024). Health app data Share with Provider FAQ. Apple Support. https://support.apple.com/guide/healthregister/health-app-data-share-with-provider-faq-apd531bc6215/web

Babu, M., Lautman, Z., Lin, X., Sobota, M. H. B., & Snyder, M. P. (2024). Wearable Devices: Implications for Precision Medicine and the Future of Health Care. Annual Review of Medicine, 75(Volume 75, 2024), 401–415. https://doi.org/10.1146/annurev-med-052422-020437

Corte-Real, A., Nunes, T., & da Cunha, P. R. (2024). Reflections about Blockchain in Health Data Sharing: Navigating a Disruptive Technology. International Journal of Environmental Research and Public Health, 21(2), 230.

Craft, L. (2024, May 2). Market Guide for Health Data Management Platforms. Gartner. https://www.gartner.com/en/documents/5399063

FAIR Institute. (2024). The Importance and Effectiveness of Cyber Risk Quantification. https://www.fairinstitute.org/what-is-fair

Fortune Business Insights. (2024, April 1). Wearable Medical Devices Market Size | Research Report [2030]. https://www.fortunebusinessinsights.com/industry-reports/wearable-medical-devices-market-101070

HealthITSecurity. (2018, July 24). How Does HIPAA Apply to Wearable Health Technology? HealthITSecurity. https://healthitsecurity.com/news/how-does-hipaa-apply-to-wearable-health-technology

Islam, M. O. U., Parah, S. A., Malik, B. A., & Malik, S. A. (2024). Lightweight medical-image encryption technique for IoMT based healthcare applications. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-024-19281-x

Kelly, B., Quinn, C., Lawlor, A., Killeen, R., & Burrell, J. (2022). Cybersecurity in Healthcare. In H. Sakly, K. Yeom, S. Halabi, M. Said, J. Seekins, & M. Tagina (Eds.), Trends of Artificial Intelligence and Big Data for E-Health (pp. 213–231). Springer International Publishing. https://doi.org/10.1007/978-3-031-11199-0_11

Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S., & Hosen, A. S. M. S. (2023). Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. Electronics, 12(9), Article 9. https://doi.org/10.3390/electronics12092050

Olsen, E. (2024, January 18). Patient records exposed in data breaches doubled in 2023. Healthcare Dive. https://www.healthcaredive.com/news/patient-records-exposed-healthcare-data-breaches-double-fortified-health-security/704917/

Murray-Watson, R. (2024, May 21). Healthcare Data Breach Statistics. *HIPAA Journal*.

OMRON Healthcare. (2024, April 30). Consumer Health Data Privacy Policy. https://omronhealthcare.com/consumer-health-data-privacy-policy/

Scarsella, A. (2024, March 24). Worldwide Smartphone Forecast, 2024–2028. IDC: The Premier Global Market Intelligence Company. https://www.idc.com/getdoc.jsp?containerId=US51916124

Singh, A. K., & Garg, A. (2024). Authentication protocols for securing IoMT: Current state and technological advancements. In D. Gupta & A. E. Hassanien (Eds.), Securing Next-Generation Connected Healthcare Systems (pp. 1–29). Academic Press. https://doi.org/10.1016/B978-0-443-13951-2.00004-0

Transform Health. (2022). The Principles: Health Data Governance Principles. https://healthdataprinciples.org/principles

Ubrani, J., Llamas, R., & Reith, R. (2024, April 2). IDC - Wearable Devices Market Insights. IDC: The Premier Global Market Intelligence Company. https://www.idc.com/promo/wearablevendor

U.S. Centers for Disease Control and Prevention. (2024, May 13). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Public Health Law. https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html

U.S. Department of Health and Human Services. (2008, May 20). Standards for Privacy of Individually Identifiable Health Information. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/standards-privacy-individually-identifiable-health-information/index.html

U.S. Department of Health and Human Services. (2021). Integrating Patient-Generated Health Data into Electronic Health Records in Ambulatory Care Settings: A Practical Guide. Agency of Healthcare Research and Quality.

U.S. Federal Trade Commission, *Health Breach Notification Rule*. 2009, pp. 476–479.

U.S. Federal Trade Commission. (2024, April 25). FTC Finalizes Changes to the Health Breach Notification Rule. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule

U.S. Office of the National Coordinator for Health Information Technology. (2017, September 15). Patient Generated Health Data | HealthIT.gov. https://www.healthit.gov/topic/health-it-health-care-settings/patient-generated-health-data

International Journal of Social Science and Public Policy

VOL: 6, ISSUE: 6
June/2024
https://ijssppnet.com/
E-ISSN: 2663-7200
http://dx.doi.org/10.33642/ijsspp.v6n6p1

Vaidya, A. (2023, February 23). Over a Third of Adults Use Health Apps, Wearables in 2023, Up From 2018. mHealthIntelligence. https://mhealthintelligence.com/news/over-a-third-of-adults-use-health-apps-wearables-in-2023-up-from-2018

Ye, J., Woods, D., Jordan, N., & Starren, J. (2024). The role of artificial intelligence for the application of integrating electronic health records and patient-generated data in clinical decision support. AMIA Summits on Translational Science Proceedings, 2024, 459–467.