Medical IoT Devices and Systems: Challenges and Opportunities

Dirceu Cavendish, Daiki Nobayashi, Takeshi Ikenaga
Faculty of Engineering
Kyushu Institute of Technology
Fukuoka, Japan
e-mail: {cavendish@net.ecs, nova@ecs, ike@ecs}.kyutech.ac.jp

***Abstract*—Rapid adoption of Internet of Things (IoT) devices within different verticals has stressed the need to strengthen security of such devices and systems. In particular, medical IoT devices must satisfy not only security, but also safety and privacy requirements. In this paper, we provide a snapshot of modern medical device systems, and underline a balanced approach to security of medical IoT systems, taking into consideration not only security risk mitigation measures but also safety and privacy of such systems. We further advocate a data driven health care delivery framework.**

***Keywords*—Medical wearables; Biosensors; Biomarkers; Personal Health Information; Risk controls; Software as a Medical Device.**

I. INTRODUCTION

The advanced state of communication networks of today has impacted many industry verticals, from financial to automotive to power transmission systems. In the medical world, the pervasive connectivity of the Internet, combined with advances in wearable sensors and data mining, is challenging traditional health care delivery models across the globe. The evolution of medical systems, however, must follow tight regulatory guardrails in order to ensure safety and privacy of patients.

In this work, we discuss challenges and opportunities of modern medical IoT devices, in this rapidly evolving "all connected" and data driven world. Specifically, we highlight security, privacy, and safety of medical IoT (m-IoT) devices. Our ultimate goal is to expose specific research areas that ultimately will enable a data driven health care delivery system.

The paper is organized as follows. Related work is included in Section II. Section III describes current medical ecosystem and its various components: Cloud, controllers, medical IoT devices, including biosensors. Section IV addresses security, safety, and privacy of medical devices and systems, with emphasis to challenges and opportunities. Section V addresses how medical data enables a novel data oriented healthcare model that benefits both healthcare providers as well as patients, via use of Artificial Intelligence/Machine Learning (AI/ML) techniques applied to healthcare. Section VI summarizes our studies and addresses promising medical IoT device research directions.

II. RELATED WORK

There has been a large proliferation of research work related to medical IoT devices recently. Most of them deal with one aspect among safety, security, privacy of these devices. For instance, Nanni et al. [1] addresses the cybersecurity vulnerabilities of medical IoT devices, providing a taxonomy as well as statistical data on various types of products. Granlund et al. [2] analyses cybersecurity and safety of medical devices from a regulatory perspective. Yaqoob et al. [3] proposes an Integrated Safety, Security, and Privacy framework to evaluate medical devices, applying it to risk evaluation of an infusion pump. They provide an excellent introduction to medical devices design controls regulated by U.S. Food and Drug Administration (FDA-US) and Medical Device Regulation (MDR-EU) regulatory bodies. Our work takes a more comprehensive approach, aiming at not only describing security, safety, and privacy aspects of m-IoT devices and system, and their interplay when comes to device requirements, but also describing specific challenges and research opportunities in realizing a data driven healthcare framework supported by a modern medical system.

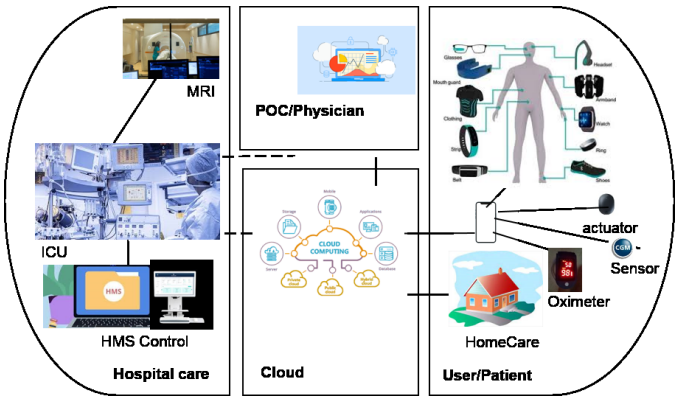

Figure 1. Modern Medical System.

III. MODERN MEDICAL SYSTEM

Figure 1 illustrates the complex medical Ecosystem nowadays. We divide the Ecosystem in four sub-systems:

- Hospital Care: Main hospital complex infrastructure, where major health procedures such as surgeries are delivered. The infrastructure contains heavy/large healthcare diagnosis and medical procedure machines, such as Magnetic Resonance Imaging (MRI) and Intensive Care Unit (ICU) Pumps. Hospital Managent System (HMS) is typically part of the infrastructure of a modern hospital.
- Point of Care (POC): This is where Physicians such as Health Care Providers (HCP) and specialists deliver healthcare services in clinics.
- Medical Cloud: This subsystem supports several medical services, from heavy machinery controls (manufacturer

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

equipment management) to physician data delivery and reports to patient data collection.
- Patient location: This subsystem encompasses patient location where care is delivered, such as a private home, or a nursing home.

Within the patient sub-system, the concept of home health care is well underway, propelled by multiple wearables and sensors currently available. In this work, we focus on sensors and wearables that are connected to HCPs, hospitals, or/end Cloud services, hereafter referred simply as medical IoT devices.

A. Current Healthcare Delivery

In most developed countries, health care is provided by a two tier system: Primary care physicians provide preventative care via patient periodic visits, typically once or twice a year, with participation of specialists once abnormality is detected; reactive care, where specialists and hospitals provide treatments for specific diseases, once detected. One problem is that preventative procedures are not always able to detect diseases at an early enough stage, decreasing probability of cure outcomes. Another issue is that the laboratory tests are performed at the snapshot time of the point of care visit. Continuous tracking of patient data, such as biomarkers (see III-B) is rarely performed.

B. Biomarkers

Biomarkers are measurable indicators of a biological state or condition. Indicators may include molecules, genes, proteins, etc. Biomarkers may be extracted from blood, urine, tissues, etc. Fig. 2 illustrates a few biomarkers.

Biomarkers can be classified according to their purpose and usage:

- Disease detection and diagnosis: Used for helping detect health conditions, even before symptoms may appear.
- Prognosis: Used for tracking severity and progression of a health condition.
- Monitoring: Used for measuring treatment response and effectiveness. Drugs side effects and consequences are managed by this type of biomarker.
- Treatment personalization: Used for tailoring to a patient a specific treatment.
- Drug development: Used for supporting clinical trials for innovative treatments.
- Risk assessment: Used for identifying individuals and group types with high chance of developing a disease.

In terms of tracking biomarkers, we differentiate between slow varying and fast varying biomarkers. Slow biomarkers may be tracked with laboratory exams few times a year. Fast varying biomarkers' readings may change significantly within few hours or days. These biomarkers require constant monitoring. Hence, biosensors is the most appropriate alternative for tracking.

Comp. Metabolic Panel (14)

Test	Current Result and Flag		Previous Result and Date		Units	Reference Interval
▲ **Glucose** [63]	**107**	**High**	95	02/25/2025	mg/dL	70-99
BUN [63]	15		19	02/25/2025	mg/dL	8-27
▼ **Creatinine** [63]	**0.72**	**Low**	**0.73**	02/25/2025	mg/dL	0.76-1.27
eGFR	105		104	02/25/2025	mL/min/1.73	>59
BUN/Creatinine Ratio	21		**26**	02/25/2025		10-24
Sodium [63]	138		138	02/25/2025	mmol/L	134-144
Potassium [63]	4.1		4.3	02/25/2025	mmol/L	3.5-5.2
Chloride [63]	103		102	02/25/2025	mmol/L	96-106
Carbon Dioxide, Total [63]	21		25	02/25/2025	mmol/L	20-29
Calcium [63]	9.1		9.0	02/25/2025	mg/dL	8.6-10.2
Protein, Total [63]	6.9		7.0	02/25/2025	g/dL	6.0-8.5
Albumin [63]	4.3		4.2	02/25/2025	g/dL	3.8-4.9
Globulin, Total	2.6		2.8	02/25/2025	g/dL	1.5-4.5
Bilirubin, Total [63]	0.8		0.9	02/25/2025	mg/dL	0.0-1.2
Alkaline Phosphatase [63]	84		76	02/25/2025	IU/L	44-121
▲ **AST (SGOT)** [63]	**55**	**High**	**66**	04/29/2025	IU/L	0-40

Figure 2. Biomarkers.

TABLE I. BIOSENSORS

Biosensor	Measures	Conditions
Oximeter [19]	Lungs oxygen saturation level heart rate	Pneumonia Blood Clots Covid-19
Glucose monitors [18]	Glucose of interstitial skin	Diabetes Obesity Insulinomia
Cholesterol monitors smart contact lenses [14]	Cholesterol in tear fluid	Hyperlipidemia Cardiovascular diseases
Electronic tattoos [17]	Heart rate Blood pressure	Cardiovascular diseases
Smartwatch/ring	steps sleep data	Sleep abnormalities

C. Biosensors

Recent development of microelectronics have made possible the design and manufacturing of several biosensors. Table I illustrates the most popular biosensors, their data and usage.

D. Data Driven Healthcare

Modern data storage systems have allowed the gathering of a multitude of health related data, whether on health care sites or in Cloud storage services [4]. In particular, data lake technologies are widely used for health care data storage.

We can classify healthcare data into few categories according to specific purposes:

- Descriptive data: Patient Health Information (PHI), such as age, gender, ethnicity; Biomarker's data 2; Environment data: patient location, work activities, workout activities (sports); Data outcomes: admission statistics; mortality rates; infection rates
- Assisted diagnosis: Databases holding specific illnesses data, to support research, diagnosis, and clinical trials. Patient anonymized data feed into data lakes. AI/Machine Learning techniques attempt to improve diagnosis time and accuracy.
- Predictive/prescriptive Analytics: Focuses on patient outcomes to diseases, mortality rate, medications' reactions and side effects. It may be used for decisions about multiple viable therapies, sometimes associated with patient genetics.

IV. Security, Safety, and Privacy of Medical Systems

In a complex medical system (Fig. 1), each component presents security vulnerabilities and security threats. In addi-

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

tion, safety threats may arise from communication issues with outside world. Finally, privacy issues may be present via data logging and hardware address information availability.

A. Edge medical devices

Device implants, such as pacemakers, require calibration, and management by an external controller. Lack of encryption and authentication between the controller and device makes it feasible the injection of harmful commands. The limited hardware and software capabilities of these devices makes it a challenge the support of a full security stack.

Biomarkers/sensors also suffer from limited hardware and software resources. Firmware authentication and secure updates are typically lacking, risking data tampering and Man In The Middle (MITM) attacks. [1] provides a taxonomy and statistical data on vulnerabilities of various wearable medical devices.

Many of these devices have as controllers applications running on smartphones, nowadays. These controllers are vulnerable to Smartphone OS vulnerabilities, tracked as Common Vulnerability Scoring System lists for specific Operating Systems (OS) versions and known vulnerabilities. Another security challenge is the lack of special security hardening OS features - essentially, medical applications are treated with the same level of security requirements as any other application on a smartphone. Typically, these medical applications lack authentication and attestation verification, even though authentication mechanisms and attestation services are available Application attestation consists in accessing the security health of an application and the device it is running at, e.g. Google Play Integrity [5].

Communication of medical sensors with controller typically takes place over Bluetooth Low Energy (BLE) wireless technology. While BLE provides a security layer, additional security protocols may be in order [6]. For instance, a medical device controller should prevent itself from pairing with a foreign BLE device. Also, a Denial of service attack may be possible if foreign controllers continually attempts to BLE pair with a medical device. Availability of hardware addresses, such as BLE MAC address may pose privacy threats if the address can be traced to user PHI information.

Finally, cryptographic material, such as certificates and cryptographic keys, needs to be protected on medical devices and sensors. One option is to use hardware areas that protect from reading/writing access outside device firmware. However, that in itself poses a challenge in lifecycle management of these cryptographic material. For instance, a medical device certificate rotation becomes difficult, especially because the medical device may not have direct connectivity to cloud services.

B. Medical Backend System

1) Medical Cloud Services: Cloud services have been growing steadily in most business areas, as attested by widely used Cloud Infrastructure such as Microsoft Azure and Amazon Web Services (AWS). From a regulatory standpoint, medical cloud services must follow the same safety, security, and privacy regulatory requirements as medical devices. However, due to the backend nature of Cloud services, the challenges are diverse from medical devices.

Modern Cloud Infrastructures have advanced security mechanisms, such as multiple cloud regions with hot backups to prevent service disruption in case of outages, load balancers with Denial Of Service preventative techniques, and gateways that arbitrate incoming and outgoing service and data transit tightly. They rely heavily on Public Key Infrastructure (PKI) certificates, which in itself requires proper management. Medical cloud services and infrastructure require design and deployment of cloud security mechanisms described above. In other words, cloud services are held to a high standard of security requirements (see IV-C).

Cloud privacy regulations [16] controls the collection of user data and its processing in the Cloud. Firstly, the principle of data minimization must be followed, which basically means that every piece of data collected must have a purpose to being gathered, and this purpose must not only be disclosed but also be consented by the user to be collected for that specific purpose. This explicit consent poses difficulties to comply with other regulatory obligations, such as post-marketing surveillance mechanisms to root cause analyze post deployment issues. A second regulatory challenge is the place at which the data is collected. Specific Cloud regions and database locations must ensure that jurisdiction boundaries are respected - collecting European user data into a US cloud region is not permitted. Another aspect of data privacy in the cloud is its capability of auditing data processing. Data access must be traceable; data accuracy must be maintained; data export to owner and to other systems (data portability) must be guaranteed. Data retention and erasure (right to be forgotten [16]) must be supported. Implementation of such tight data control features by the cloud poses many practical challenges.

2) Hospital Infrastructure: Hospital infrastructure typically houses ”legacy” equipment with obsolete Operating Systems that contain plenty of well known vulnerabilities. In addition, many such equipment have hardcoded credentials and no strong data encryption/protection, allowing for outside cyber break in, code injection, and ultimately ransomware attacks. These legacy equipment must be isolated from connectivity with other sub-systems and the Internet, if possible. A hospital management system may provide isolation of sub-systems. In addition, it must support a strong Identity and Access Management (IAM) service, with PHI and medical data access on a strictly and per needed basis.

C. Medical Device Regulatory Landscape

1) Medical Devices Safety: Medical devices' safety are tightly regulated by international standards, from design until end of life. [7] specifies a quality management system for the design, verification and validation of medical devices. It mandates a thorough documentation of the design process, from requirements to their verification and validation. Such documentation is referred to as Design History Files, and it is auditable by regulatory bodies such as FDA in the United

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

States. In addition, [8] specifies a risk management procedure where safety risks are identified, quantified, and mitigated during the design of medical devices.

Still within patient's safety, [12] and [13] address software risks impacting patient's health.

2) Medical Devices Security: Medical device security framework leverages various general security standards, governed by security organizations such as National Institute of Standards and Technology (NIST). Specific to medical devices, [9] describes a framework to access cybersecurity risks associated with medical devices. In addition, [10] describes an approach to conduct risk assessments. Finally, [11] provides a framework to track and manage security vulnerabilities of networked devices.

3) Medical Devices Privacy: The two major regulation standards on privacy are Health Insurance Portability and Accountability Act (HIPPA) [15] and General Data Protection Regulation (GDPR) [16] in the United States and Europe, respectively. These standards define Personal Health Information (PHI) as any data that may be traced to an individual identity, and attempt to protect such data from misuse. In particular, GDPR privacy framework brings transparency to medical data owner regarding their medical data collection and processing. The privacy framework mandates user consent in the usage of such data, and further supports user right to a copy of their data, as well as its deletion, referred to as right to be forgotten. In addition, the framework calls for anonymization techniques to protect user privacy, as well as minimization of data collection, forbidding data gathering without specific purposes consented by the user.

As mentioned before, modern networked medical devices must protect information exported to controllers and Cloud infrastructure from privacy threats. For instance, hardware addresses such as MAC address must be at a minimum obfuscated if it needed to be exported outside the device.

4) Balancing Regulatory Standards: Although compliance with all three regulatory areas, safety, security, and privacy is the ultimate goal, requirements in different areas are sometimes conflicting,as represented in Fig. 3. The overlapping areas of the ovals represent non-conflicting requirements. One can see that only a small set of requirements may be aligned across all three areas.

Examples of tradeoff are:

- A pacemaker controller that has been detected to be security compromised may be required to remain in connection to the pacemaker until a suitable replacement or security fix may be available, for patient safety. In essence, therapy interruption may be more dangerous to the patient than allowing operation upon a security issue detection.
- Device ID/address (such as Media Access Control - MAC address) may be required to be collected, despite privacy concerns, in order to mitigate risk hazards, or security threats, such as connecting to a foreign medical device.

We advocate an integrated risk management system, as per

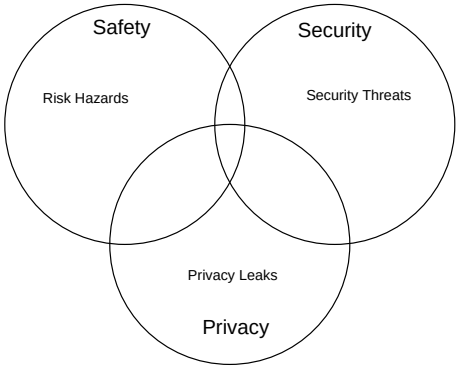

Figure 3. Safety, Security, And Privacy Risks.

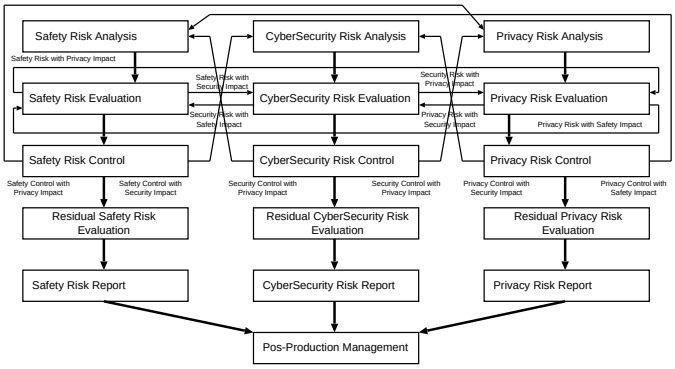

Figure 4. Integrated Risk Methodology.

Fig. 4, extending International Organization for Standardization (ISO) 14971 [8] into cybersecurity and privacy areas.

The figure displays how safety, cybersecurity and privacy risks must be evaluated in a cross impact manner. It also calls for residual risk analysis taking into account cross area risk controls. A Bayesian framework, similar to the one proposed in [3] may be used to quantify hazard probabilities and risk evaluation.

V. Medical Data Oriented Healthcare

Recent advances in medical data collection and large data processing are pushing health care delivery into a new data driven paradigm. Today, physicians and nurses are able to track patients medical data multi-day evolution via Cloud services. In addition, today Cloud data collection may be combined with advanced data processing techniques in search for abnormalities. We then may conceive a health care model at which physician's visit may be triggered by cloud services notifications directly from a patient to the physician's office. For instance, blood glucose can be tracked to detect pre-diabetes condition, and correlated with other data such as patient weight and Body Mass Index (BMI). This personalized data driven diagnoses allows a more preventative health care model, rather than a reactive model where medical data is obtained only upon symptoms appearance. Challenges to build a data driven diagnosis system is that physician's workflows may be different, depending on the specialty and nature of the

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

disease. For instance, an orthopedic joint problem typically requires some imaging processing, where oncology conditions may be detected by extensive lab tests.

In addition to diagnosis, illnesses treatment decision may be driven by tracking specific drugs' side effects within a large patient population, as well as treatment's effectiveness within a group of patients with similar genetic and environmental characteristics. Machine learning techniques, such as clustering, may help with data driven diagnosis and treatment decisions.

At the heart of this data driven healthcare framework is AI/ML models that must be able to accurately process a large amount of data. In this section, we call AI/ML medical products as Software as a Medical Device (SaMD). As with any other medical device, the manufacturer needs to seek approval from regulatory bodies such as FDA and MDR, which requires proof of safety and effectiveness of the SaMD. The self-learning characteristics of such devices make it non-trivial to show safety and effectiveness, and regulatory agencies are still grappling to define methods and procedures for SaMD submissions.

As a baseline, AI/ML SaMD must describe their training sets, their size and diversity so as to perform well when dealing with a diverse patient population. As far as effectiveness is concerned, SaMD may intend to provide assistance to a physician only, for instance, in diagnosis within a specific specialty (see [20] for use cases). In that respect, efficacy may be measured by how fast the physician came to the correct diagnosis when aided by the SaMD, as opposed to doing it alone. This is in sharp contrast to non-learning medical devices, where efficacy is oftentimes proved by comparison with equivalent devices in the market. Finally, in terms of safety, medical devices with learning capabilities must include safeguards in case the learning process goes awry. For instance, a smart ICU pump should support maximum drug delivery rates, so as not to endanger patient's life.

As clinical trials are part of regulatory approval process, specific procedures to accommodate learning mechanisms should be devised for SaMDs [21].

VI. Conclusion and Future Work

In this paper, we have addressed safety, security, and privacy aspects of modern medical systems and their components, with emphasis to medical IoT devices, such as biosensors. We have exposed challenges of modern medical IoT devices security and privacy, vis a vis ensuring user safety. Furthermore, we have argued for a balanced approach in analyzing device risks and risk controls. We have also underlining the challenges in proving the safety and effectiveness of medical devices that make use of AI/ML mechanisms.

Specific topics of research for medical devices include: reliable source of time; authentication and secure communication; secure firmware updates; AI guardrail framework. We are currently investigating some security aspects of medical devices with impact on user privacy and safety.

Acknowledgments

Work supported by JSPS KAKENHI Grant #24K03045.

References

[1] F. M. C. Nanni et al., "Taxonomy and Statistics of Cyber and Physical Vulnerabilities in Medical Devices," 9th International Conference on Smart and Sustainable Technologies - SpliTech, Digital Object Identifier 10.23919/SpliTech61897.2024.10612327, June 2024.

[2] T. Granlund et al., "On Medical Device Cybersecurity Compliance in EU", IEEE/ACM 3rd International Workshop on Software Engineering for Healthcare (SEH), pp. 20-23, 2021.

[3] T. Yaqoob and H. Abbas, "Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices," IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 6, pp. 1752-1761, June 2020.

[4] A. Ahmed et al., "Harnessing Big Data Analytics for Healthcare: A Comprehensive Review of Frameworks, Implications, Applications, and Impacts," IEEE Access, Digital Object Identifier 10.1109/ACCESS.2023.3323574, Oct.2023.

[5] Android Developers, "Google Play Integrity", URL: https://developer.android.com/google/play/integrity/overview, last accessed Oct. 19, 2025 (UTC).

[6] A. Barua et al., "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," IEEE ComSoc, Digital Object Identifier 10.1109/OJCOMS.2022.3149732, Feb.2022.

[7] ISO 13485: 2003, Medical devices – Quality management systems.

[8] ISO 14971: 2019, Medical devices – Application of risk management to medical devices.

[9] IEC 80002-1: 2009, Medical device software — Part 1: Guidance on the application of ISO 14971 to medical device software,https://www.iso.org/standard/54146.html, last accessed Nov. 29, 2025.

[10] NIST SP 800-30 Rev. 1 Guide for conducting risk assessment, https://csrc.nist.gov/pubs/sp/800/30/r1/final,last accessed Nov. 29, 2025.

[11] IEC/TS 81001-2-2:2025 Health software and health IT systems safety,effectiveness, and security Part 2-2: Guidance for the implementation, disclosure and communication of security needs, risks and controls https://www.iso.org/standard/85765.html, last accessed Nov. 28, 2025.

[12] IEC 62304: 2006, Medical device software — Software life cycle processes, https://www.iso.org/obp/ui/iso:std:iec:62304:ed-1:v1:en,last accessed Nov. 16, 2025.

[13] IEC 82304: 2016, Health software — Part 1: General requirements for product safety, https://www.iso.org/obp/ui/en/iso:std:iec:82304:-1:ed-1:v1:en, last accessed Nov. 16, 2025.

[14] H. Song et al., "Wireless Non‐Invasive Monitoring of Cholesterol Using a Smart Contact Lens," https://onlinelibrary.wiley.com/doi/10.1002/advs.202203597, last accessed Jan. 18, 2026.

[15] U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/index.html, last accessed Nov. 16, 2025.

[16] General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Directive 95/46. Official Journal of the European Union (OJ), 2016, vol. 59, no. 1-88, p. 294.

[17] K. Sel et al., "Electrical Characterization of Graphene-based e-Tattoos for Bio-Impedance Physiological Sensing," IEEE Biomedical Circuits and Systems Conference (BioCAS), Print on Demand, Oct., 2019.

[18] S.A.Siddiqui et al., "Pain-Free Blood Glucose Monitoring Using Wearable Sensors: Recent Advancements and Future Prospects," IEEE Reviews in Biomedical Engineering, Vol. 11, pp. 21-35, Apr., 2018.

[19] M. A. Motin et al., "Compact Pulse Oximeter Designed for Blood Oxygen Saturation and Heart Rate Monitoring," 3rd Int. Confrence on Electrical & Electronic Engineering (ICEEE), pp. 125-128, Dec. 2021.

[20] S. Ahmed, J. Y. Raja, M. Y. A. Raja, "eHealthcare: IoT & AI Enhance the Scope and Effectiveness of Diagnostics and Treatment Modalities", IEEE 21st International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET), pp. 156-161, 2024.

[21] S-R Yang, J-T Chien, and C-Y Lee, "Advancement in Clinical Evaluation and Regulatory Frameworks for AI-Driven Software as a Medical Device," IEEE Open Journal of Engineering in Medicine and Biology, vol. 6, pp. 147-151, 2025.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org