Assessing Privacy and Security Compliance in Urinary Incontinence Wearable Devices

Amina Bouayed*, Johannes C. Ayena*, Myriam Ben Arous*, Youssef Ouakrim*, Karim Loulou*, Leila El Kamel*
Habib Louafi† and Neila Mezghani*

*Applied Artificial Intelligence Institute (I2A), TELUQ University
5800 St Denis, Montreal, Qc., H2S 3L4, Canada
email: amina.bouayed@gmail.com; johannes.ayena@teluq.ca; myriam.ben.arous@umontreal.ca;
youssef.ouakrim@teluq.ca; karim.loulou@teluq.ca; leila.elkamel@teluq.ca; neila.mezghani@teluq.ca

†Science and Technology, TELUQ University
5800 St Denis, Montreal, Qc., H2S 3L4, Canada
email: habib.louafi@teluq.ca

***Abstract*—Wearable devices have revolutionized healthcare by providing innovative solutions for managing medical conditions such as urinary incontinence (UI). However, despite their effectiveness, these technologies face significant cybersecurity and data privacy concerns, particularly the protection of sensitive health information. In this paper, we examine various UI detection and prevention devices, focusing on their compliance with critical cybersecurity and privacy regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and industry standards, including ISO 13485 and ISO 27001. Our findings reveal that while some devices display certifications, such as CE marking or FDA approval, important security and compliance information are often unclear, inaccessible, or missing. To mitigate risks, manufacturers must not only secure wireless communication protocols but also prioritize transparency regarding their adherence to legal and industry requirements to safeguard user data. This study highlights the urgent need for clear guidelines on security and privacy compliance to ensure an ethical integration of wearable device technologies into UI healthcare systems, and safeguarding sensitive patient data such as UI severity, frequency of urinary leakage, and other key parameters.**

***Index Terms*—urinary incontinence, privacy, assessment, end-users, market access**

I. Introduction

Urinary Incontinence (UI), characterized by the involuntary loss of urine, has attracted significant scientific interest over the past decade [1]. Studies across various countries indicate that 5–70% of the population is affected, with a higher prevalence among women [2]. UI not only causes personal suffering (social isolation, depression, feelings of loneliness, reduced quality of life, etc.) but also generates major economic expenses for healthcare services [3]. While conventional approaches, including lifestyle changes, pelvic floor muscle training, bladder training, and medication, remain viable options [4], multiple surgical solutions such as Burch surgery, midurethral sling, and pubovaginal sling [5] are also available. However, they are often associated with high complications and complex procedures [6].

In recent years, technological advancements have introduced some smart wearable devices as a promising alternative for UI management [7], [8]. These devices offer continuous bladder state monitoring, improve adherence to training programs, and enhance self-management support [9]. However, their integration into healthcare systems presents significant cybersecurity and data privacy challenges. Indeed, these devices continuously collect and transmit sensitive health data often via wireless communication protocols to cloud-based or on-premise storage raising concerns about data breaches, unauthorized access, and regulatory compliance [10]. Ensuring the confidentiality, integrity, and availability of this data is crucial, since failing to do so could result in severe legal and ethical consequences, including privacy violation and potential cyberattacks [10], [11]. To address these risks, wearable devices must comply with data protection regulations and industry standards such as the General Data Protection Regulation (GDPR), the EU Data Act, and the Health Insurance Portability and Accountability Act (HIPAA) [12]–[14]. These regulatory frameworks establish essential guidelines for securing wireless communications, implementing encryption protocols, and enforcing data access controls. Compliance with these standards not only mitigates security vulnerabilities but also enhances user trust in wearable healthcare technologies.

To the best of our knowledge, no previous work has yet comprehensively examined the compliance, cybersecurity, and

This research was supported by the Programme Audace Plus—Fonds de recherche du Québec—FRQ and the Canada Research Chair on Biomedical Data Mining (950-231214).

data privacy aspects of wearable devices for UI, particularly in terms of compliance with regulatory standards such as GDPR, HIPAA, ISO 13485 and ISO 27001. Our study addresses this gap by evaluating the compliance of existing UI-related devices with critical regulations and emphasizing the need for clear cybersecurity guidelines to protect sensitive patient data. We believe that our findings will help to inform clinical practices, guide consumer decisions, and highlight areas for future security improvements in UI-related wearable technology.

The paper is structured as follows: Section II details the methodology, which follows a systematic review approach to retrieve UI wearable devices. Section III presents an overview of some UI wearable devices, showing their characteristics, security considerations, and regulatory compliance. Section IV provides a discussion of these findings, highlighting significant observations, existing security standards, emerging risks, and potential directions for further research and development. Finally, Section V summarizes the main insights and implications of the study.

II. Methodology

This study investigates commercially available wearable devices for UI, focusing on their functionalities, targeted users, ethical considerations, and compliance with privacy and cybersecurity regulations. Unlike research prototypes [7], [8], which rarely face real-world deployment, commercial devices are actively used in healthcare settings and manage sensitive patient data. Evaluating these products is therefore crucial to identify regulatory gaps and assess practical risks. This is addressed through a structured systematic review.

A. Research Question and Search Strategy

Our research is guided by the following questions:

- What are the current encryption and authentication mechanisms used in UI wearable devices and how effective are they in protecting sensitive health data that is collected, processed, and eventually transmitted?
- What are the most common cybersecurity vulnerabilities in wireless communication of UI wearable devices, and how can they be mitigated?
- How do firmware update mechanisms and access control policies impact the overall security and resilience of UI wearable devices against cyber threats?
- What are the challenges in ensuring compliance of UI-related devices with healthcare data privacy regulations (e.g., HIPAA, GDPR), while maintaining their usability and accessibility for users?

To answer these questions, we exploited the search strategy and results from our previous systematic review presented in [7] which used four databases (PubMed, IEEE Xplore, Web of Science, Scopus). Additionally, we used Google Scholar to expand the search scope by adding more specific terms, including FDA cleared, regulations, etc. To ensure a comprehensive market overview, we also examined manufacturer websites, regulatory agency databases (e.g., FDA, European Medical Device Regulation), and commercial product listings. Therefore, the new search strategy, incorporating keywords and Boolean operators, was set as follows as: (”urinary incontinence” OR ”bladder monitoring”) AND (”non-invasive” OR ”wearable device*” OR ”smart diaper”) AND (”detection” OR ”prevention”) AND (”commercial” OR ”marketed”).

B. Selection Criteria

Only commercially available wearable UI devices were considered, particularly those integrating sensors, wireless connectivity, and mobile app support for monitoring and managing incontinence. Selected devices should possess regulatory certifications such as CE marking, FDA approval, or compliance with ISO standards, to ensure safety and effectiveness. Additionally, products should provide privacy and security measures, including data encryption and/or compliance with GDPR or HIPAA standards. Devices designed solely for general pelvic health or lacking wearable components (e.g., traditional catheter-based solutions) were excluded.

C. Data Extraction

For each selected wearable UI device, relevant data was systematically extracted to evaluate its functionality, targeted audience, ethical considerations, and legal compliance. Main attributes include device type, sensor technology, wireless communication protocols, data storage methods (cloud or local), and intended users (patients or healthcare providers). Additionally, information related to privacy policies, encryption mechanisms, regulatory certifications (e.g., GDPR, HIPAA, ISO 13485, ISO 27001, CE marking, FDA approval), and manufacturer transparency was collected. Data sources included peer-reviewed studies, official product documentation, regulatory agency reports, and manufacturer websites.

III. Results

In our study, we identified eight wearable devices that are currently available for UI detection and prevention. These devices and their characteristics are presented in Table I. Each device is categorized based on its UI application type (detection or prevention), targeted population, underlying sensor or technology, core functionalities or features, and its

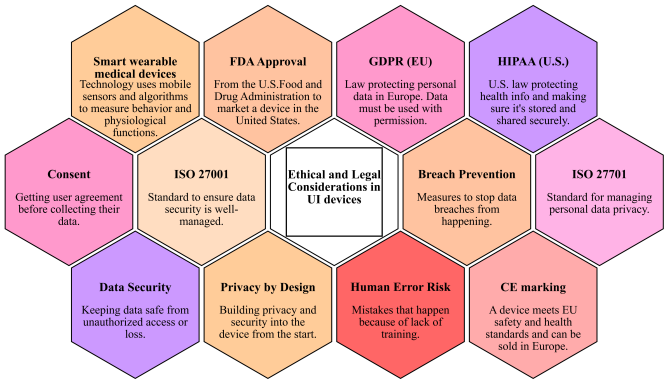

Fig. 1: Key terms for ethical, legal, and technical considerations in the design of UI Devices. Note that the definitions are from diverse sources [12], [14]–[17].

TABLE I: Overview of Selected and Analyzed Smart Wearable Devices for UI Detection and Prevention

Detection							
Device Name	**Population**	**Sensor/Technology**	**Functionality**	**Advantages**	**Disadvantages**	**Medical**	**Compliance**
STOPEE [18]	4–18 yrs	Sensor pad	Detects moisture via electrical change; triggers alarm on first drops	Learning software, volume control, detects small amounts	Expensive, requires additional monitoring	Y	CE, FDA (no info on data security)
Opro9 [19]	Adults, Babies	Temperature, Humidity	Diaper moisture alerts via Bluetooth	Reusable, fits all diapers, alerts via phone	Detects only after urine enters diaper	N/A	ISO certified (standard unspecified)
Monit Smart Baby [20]	0–3 yrs	Temperature, Humidity, Pressure, Accelerometer, Gas sensor	Detects wetness via humidity and temperature changes; Bluetooth alerts	Works with all diapers, Bluetooth-enabled	Requires charging, mainly for medical use	N/A	CE marked
Monit Elderly Care [20]	Elderly	Temperature, Humidity, Pressure, Accelerometer, Gas sensor	Detects wetness via humidity and temperature changes; Bluetooth alerts	Compatible with all diaper types; connects via Bluetooth through a mobile app; supports multiple functions like fall detection and posture analysis	Charges through a dedicated station (sold separately); Primarily intended for medical personnel	N/A	CE marked
Smardii [21]	Adults, Children	Disposable sensor strips	Real-time wetness alerts via app	Fall detection, geolocation	Designed for medical personnel	Y	GDPR
Lumi by Pampers [22]	Babies	Temperature, Accelerometer	Detects wetness using Lumi diapers via Bluetooth	Small, energy-efficient	Works only with Lumi diapers	N/A	N/A
Prevention							
Device Name	**Population**	**Sensor/Technology**	**Functionality**	**Advantages**	**Disadvantages**	**Medical**	**Compliance**
DFree [23]	UI patients Seniors	Ultrasonic sensors	Detects bladder fullness; sends alerts via app	Non-invasive, real-time monitoring, long battery life	Expensive, privacy concerns, potential inaccuracies	N	N/A
SENS-U [24]	6–16 yrs	Ultrasonic sensors	Monitors bladder filling; alerts via phone	Real-time, non-invasive	Discomfort from wear, false alarms, expensive	Y	CE, FDA, ISO 13485

Note: N/A means 'Not Available', Y means 'Yes', N 'No', GDPR: General Data Protection Regulation, UI: Urinary Incontinence, CE for European Conformity, FDA stands for the U.S. Food and Drug Administration, ISO International Organization for Standardization.

respective advantages and disadvantages. In addition, we indicate whether each device is classified as a medical device or not (Fig. 1). Finally, the device compliance with relevant regulatory standards is also reported.

A. Features and Conceptual Clarification for UI Devices

Fig. 1 presents critical definitions of some terms to ensure clarity and understanding of the concepts involved in ethical and legal considerations of UI devices. Updates on these terms are essential, as they enable readers, with varied prior knowledge, to fully understand the technical, ethical, and legal elements involved. By providing clear definitions, we eliminate potential ambiguities and ensure that the context of devices is understood consistently, which is particularly important when addressing complex concepts, such as regulatory compliance, data privacy and device functionality and features related to urinary incontinence.

B. Compliance with Regulatory and Cybersecurity Standards

STOPEE and SENS-U meet CE and FDA requirements [18], [25], with SENS-U manufacturer is also certified under ISO 13485 for medical device management system. However, neither provides specific details on data security protocols they implement. Smardii claims compliance with GDPR [21],

but its available documentation lacks transparency in several important areas. Indeed, there is no clear explanation of what personal data is collected, the legal basis for processing it, or how long the data is retained. Additionally, there is no mention of whether data is shared with third parties or transferred internationally nor how users can exercise their data rights. Notably, Smardii does not provide evidence of certification, independent audits, or adherence to recognized data protection standards raising concerns about how seriously it takes its commitment to personal data safety and compliance. Opro9 manufacturer is ISO-certified [26], though the specific standard remains unclear, and no information is provided on GDPR or HIPAA compliance. Monit holds a CE marking but does not disclose any data privacy measures [20], [27]. DFree is not a certified medical device, and its unreliable Bluetooth connection raises potential security concerns [28].

C. Communication Security and Vulnerability Risks

Most analyzed devices rely on Bluetooth (Table I), which is known as a vulnerable and unstable protocol, for data transmission, introducing risks of interception or hacking [29]. DFree, in particular, has been reported for its unstable connectivity, which could compromise real-time notifications [30]. Furthermore, no details are provided regarding encryption protocols or authentication mechanisms, raising concerns about data protection during transmission. The absence of information on security audits or penetration testing further highlights potential cybersecurity weaknesses in these devices.

D. Transparency on Handling of Sensitive Data

Most manufacturers provide little to no information on data storage, processing, and deletion policies (Table I). None of the analyzed devices mention security audits or compliance with ISO 27001/27701, which are essential for secure data management. While Smardii claims GDPR compliance, it does not specify how user data is protected or how users can control their personal information [21]. Additionally, the lack of clear encryption standards increases the risk of unauthorized access to sensitive health data. Lack of information about compliance with regulations or industry standards for data security increases the likelihood of cybersecurity risks. These risks include data privacy, breaches and unauthorized access to personal data, interception of data transmissions that generate false results, and more.

IV. Discussion

Wearable devices for the UI treatment offer innovative solutions to improve patient well-being through continuous monitoring and personalized notifications. However, their development and use raise significant concerns regarding legal, ethical and data security and privacy aspects, which vary considerably from device to device.

A. Implications of Cybersecurity in UI Devices

UI devices are connected devices using Bluetooth or other protocols for data transmission. Most of those devices' provided results are shown in a mobile or web application. The transmission of data is the most vulnerable phase in this process, as the protocol in use can easily be hacked and data intercepted if no strong security measures (e.g., encryption) are implemented [29]. Besides, those devices also store data locally for interpretations and significant analysis, such as bladder activity, urine frequency, etc [8]. Data storage is also a vulnerable step in the process if the storage method (cloud or in-premise) is not well designed and secured. Regulations and industry cybersecurity standards help manufacturers implement adequate measures to prevent data security and privacy risks, not only across the entire infrastructure, but also at the device level.

From a legal point of view, many of these devices (Table I) lack full regulatory compliance. While some, such as STOPEE and SENS-U, benefit from CE marking and FDA approval [18], [25], others, such as Opro9 and MONIT, do not offer sufficient transparency on their compliance with key regulations, such as GDPR or HIPAA [26], [27]. The lack of clear information on data protection measures highlights a gap in legal compliance, particularly when handling sensitive health data. Ethically, the collection and processing of health data by these devices requires robust and transparent frameworks to protect user privacy [10]. Devices like Smardii claim to be GDPR-compliant, but the lack of detailed documentation leaves questions about their implementation. The ethical responsibility of manufacturers to ensure informed consent, transparency and the right to access and delete data is only partially addressed in the devices reviewed.

Data security remains another crucial challenge. As stated earlier, many devices use Bluetooth for communication, a vulnerable technology [31], as evidenced by DFree's reported problems. Furthermore, no device demonstrates compliance with industry standards, such as ISO 27001 or ISO 27701, which are essential for implementing effective security measures [32]. For example, although SENS-U is ISO 13485 certified for medical devices, it lacks certifications dealing

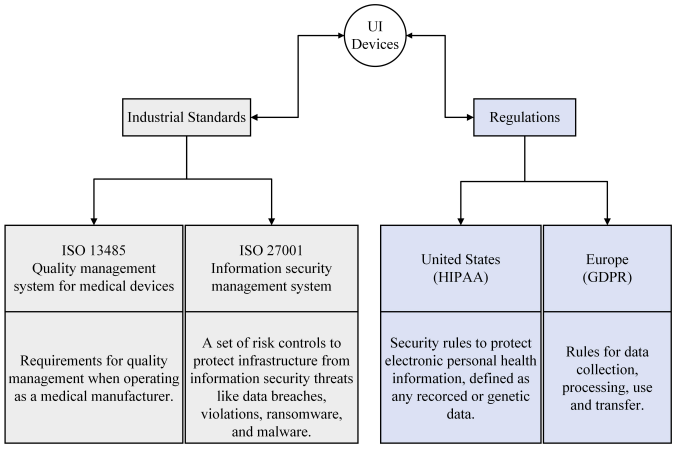

Fig. 2: Fundamental compliance standards and regulations relevant to UI device development. Note that GDPR means General Data Protection Regulation, UI Urinary Incontinence, HIPAA Health Insurance Portability and Accountability Act, ISO International Organization for Standardization.

specifically with data confidentiality and security.

B. Limitations of the Study

This study is limited by lack of transparency on compliance. Most of the devices do not provide any information about this issue. A comprehensive comparison of all UI healthcare devices is still needed to better support consumer decision-making and advance research on security and privacy compliance. While these devices are promising for improving healthcare, their large adoption depends on addressing the legal, ethical, and safety issues that have been identified. Manufacturers should prioritize compliance with global regulations, adopt recognized data protection standards, and enhance transparency to build user trust and ensure safe integration of these technologies into healthcare systems.

C. Future Directions and Recommendations

A device designed to address UI, whether considered a medical device or not, shall follow a set of practices, standards or regulations to maximize its performance in terms of information security and users' privacy. This compliance allows users to responsibly handle their personal data, such as intentional or unintentional personal data storage, processing, and sharing. Fig. 2 presents fundamental compliance standards and regulations, which we believe every device should be compliant with a least one of them. In addition, all manufacturers must be transparent on how these standards are implemented and how data can be handled, by providing clear and easy to read data handling protocols. To ensure accountability, they should adopt recognized standards such as ISO/IEC 27001 for security, GDPR for data protection in Europe, and HIPAA for health data in the U.S. These frameworks help secure user data and uphold privacy rights.

V. Conclusion

Wearable devices offer valuable solutions for managing urinary incontinence. However concerns about data privacy and security remain. A comprehensive comparison of devices is still needed to support informed consumer choices and ensure compliance with regulations like GDPR and HIPAA. Greater transparency in security measures is essential to safeguard patient data and build confidence.

References

[1] A. Rantell, "Tackling the stigma of incontinence," in *Textbook of Female Urology and Urogynecology*, pp. 10–16, CRC Press, 2023.

[2] I. Milsom, D. Altman, R. Cartwright, M. Lapitan, R. Nelson, U. Sillén, and K. Tikkinen, *Epidemiology of Urinary Incontinence (UI) and other Lower Urinary Tract Symptoms (LUTS), Pelvic Organ Prolapse (POP) and Anal Incontinence (AI)*, pp. 15–107. France: ICUD-EAU, 5th ed ed., 2013.

[3] K. Zehra and E. Aslan, "The burden and cost in urinary incontinence," *The New Journal of Urology*, vol. 16, no. 1, pp. 79–88, 2021.

[4] A. I. Mazur-Bialy, D. Kołomańska-Bogucka, C. Nowakowski, and S. Tim, "Urinary incontinence in women: modern methods of physiotherapy as a support for surgical treatment or independent therapy," *Journal of clinical medicine*, vol. 9, no. 4, p. 1211, 2020.

[5] B. C. Călinescu *et al.*, "Surgical treatments for women with stress urinary incontinence: A systematic review," *Life*, vol. 13, no. 7, p. 1480, 2023.

[6] N. Mangir, S. Roman, C. R. Chapple, and S. MacNeil, "Complications related to use of mesh implants in surgical treatment of stress urinary incontinence and pelvic organ prolapse: infection or inflammation?," *World Journal of Urology*, vol. 38, pp. 73–80, 2020.

[7] M. B. Arous *et al.*, "Non-invasive wearable devices for urinary incontinence detection—a mini review," *Frontiers in Sensors*, vol. 4, p. 1279158, 2023.

[8] M. Z. Nasrabadi, H. Tabibi, M. Salmani, M. Torkashvand, and E. Zarepour, "A comprehensive survey on non-invasive wearable bladder volume monitoring systems," *Med Biol Eng Comput*, vol. 59, pp. 1373–1402, 2021.

[9] A. Hafid *et al.*, "State of the art of non-invasive technologies for bladder monitoring: a scoping review," *Sensors*, vol. 23, no. 5, p. 2758, 2023.

[10] C. Elendu, E. K. Omeludike, P. O. Oloyede, B. T. Obidigbo, and J. C. Omeludike, "Legal implications for clinicians in cybersecurity incidents: A review," *Medicine*, vol. 103, no. 39, p. e39887, 2024.

[11] D. J. Solove and W. Hartzog, *Breached!: Why data security law fails and how to improve it*. Oxford University Press, 2022.

[12] Afnor Certification, "Marquage CE dispositif médical." https://certification.afnor.org/en/quality/ce-marking-for-medical-devices.

[13] P. F. Edemekong, P. Annamaraju, and M. J. Haydel, "Health insurance portability and accountability act," 2018.

[14] Official Journal of the European Union, "General data protection regulation." https://eur-lex.europa.eu/eli/reg/2016/679/oj, 2016.

[15] P. F. Edemekong *et al.*, "Health insurance portability and accountability act," 2018.

[16] J. C. Goldsack *et al.*, "Verification, analytical validation, and clinical validation (v3): the foundation of determining fit-for-purpose for biometric monitoring technologies (biomets)," *npj digital Medicine*, vol. 3, no. 1, p. 55, 2020.

[17] E. Lachaud, "Iso/iec 27701 standard: Threats and opportunities for gdpr certification," *European Data Protection Law Review*, vol. 6, p. 194, 2020.

[18] Therapee by Dr Sagie, "The world's 1 bedwetting solution." https://www.bedwettingtherapy.com/.

[19] Opro9, "Smart diaper." https://www.cvicloud.com/smartdiaper/.

[20] MonitCorp, "Monit Smart Baby Monitor." https://www.tradekorea.com/product/detail/P770551/MONIT-Smart-baby-monitor.html.

[21] Smardii Inc., "Making critical health data available to caregivers." https://www.smardii.com/.

[22] WFLA News Channel 8, "Lumi by pampers smart baby monitor review." https://www.youtube.com/watch?v=82WPxv6WzJs, 2025.

[23] Triple W., "Dfree." https://www.dfreeus.biz/.

[24] Novioscan Inc., "Sens-u kids." https://novioscan.com/.

[25] Novioscan Inc., "About novioscan." https://novioscan.com/about/.

[26] Opro9, "Catalogue for your intelligent life." https://www.opro9.com/wp-content/uploads/2020/08/2020-Opro9-Smart-Home-Issue-en-vol2-v1-20200520-compress.pdf.

[27] MonitCorp, "Digital healthcare for the loved one." https://www.monitcorp.com/en/mecs.

[28] H. Strauven, V. Vanden Abeele, H. Hallez, and B. Vanrumste, "Supporting continence care management in nursing homes via a toilet timing predicting wearable," in *ICS 2020, Date: 2020/11/19-2020/11/22, Location: Las Vegas*, 2020.

[29] T. Ali, R. Baloch, M. Azeem, M. Farhan, S. Naseem, and B. Mohsin, "A systematic review of bluetooth security threats, attacks & analysis," *International Journal of Computer Trends and Technology*, vol. 69, no. 7, pp. 1–18, 2021.

[30] S. Hofstetter *et al.*, "Dfree ultrasonic sensor in supporting quality of life and patient satisfaction with bladder dysfunction," *International Journal of Urological Nursing*, vol. 17, no. 1, pp. 62–69, 2023.

[31] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, "Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 251–281, 2022.

[32] E. Lachaud, "Iso/iec 27701 standard: Threats and opportunities for gdpr certification," *Eur. Data Prot. L. Rev.*, vol. 6, p. 194, 2020.