Envisioning Secure and Private 6G-Enabled Cognitive Personal Informatics

Anna Triesch
anna@aware7.de
AWARE7 GmbH
Germany

Jan Hörnemann
jan@aware7.de
AWARE7 GmbH
Germany

Tobias Urban
urban@internet-sicherheit.de
Institute for Internet Security, Westphalian University of Applied Sciences
Germany

Matteo Große-Kampmann
matteo.grosse-kampmann@hochschule-rhein-waal.de
Rhine-Waal University of Applied Sciences, AWARE7 GmbH
Germany

ABSTRACT

This Paper explores how emergent technologies such as 6G and tactile Internet can potentially enhance cognitive, personal informatics (CPI) in participatory healthcare, promoting patient-centered healthcare models through high-speed, reliable communication networks. It highlights the transition to improved patient engagement and better health outcomes facilitated by these technologies, underscoring the importance of ultra-reliable, low-latency communications (URLLC) and realizing the tactile Internet's potential in healthcare. This innovation could dramatically transform telemedicine and mobile health (mHealth) by enabling remote healthcare delivery while providing a better understanding of the inner workings of the patient. While generating many advantages, these developments have disadvantages and risks. Therefore, this study addresses the critical security and privacy concerns related to the digital transformation of healthcare. Our work focuses on the challenges of managing and understanding cognitive data within the CPI and the potential threats from analyzing such data. It proposed a comprehensive analysis of potential vulnerabilities and cyber threats, emphasizing the need for robust security frameworks designed with resilience in mind to protect sensitive cognitive data. We present scenarios for reward and punishment systems and their impacts on users. In conclusion, we outline a vision for the future of secure, resilient, and patient-centric digital healthcare systems that leverage 6G and the tactile Internet to enhance the CPI. We offer policy recommendations and strategic directions for stakeholders to create a secure, empowering environment for patients to manage their cognitive health information.

KEYWORDS

6G, Security, CPI

1 THE PROMISE OF 6G AND TACTILE INTERNET IN COGNITIVE PERSONAL INFORMATICS

Advancements in wearable neurotechnologies and activity monitors are paving the way for the continuous measurement, quantification, analysis, and interpretation of cognitive functions, mirroring the enhancement of physical health through similar devices [4, 14]. Presently, efforts to categorize cognitive functions using wearable and ambient technologies are at a stage of development comparable to physical activity monitoring in the early 2000s. CPI is particularly promising when combined with 6G and the tactile Internet. This integration can significantly enhance patient engagement and satisfaction by providing real-time insights into cognitive well-being, thereby enabling personalized and responsive healthcare interventions. For instance, mobile health (mHealth) applications can deliver cognitive behavioral therapies tailored to individual patient needs, monitor cognitive load to prevent burnout and provide cognitive rehabilitation services with real-time feedback within a patient's natural environment [36]. Consumers now have the option to purchase specialized devices aimed at monitoring brain activity, which monitor brain activity and measure lactate levels via in-ear sensors [38]. In addition, some wearables claim to gauge stress levels by monitoring respiratory patterns[1], bracelets that adapt to recognize individual emotional trends[2], and watches that suggest activities to regulate physiology, such as guided breathing for improved well-being[3]. Moreover, gadgets that track sleep patterns and assess mental preparedness for upcoming tasks are also available [15]. The Tactile Internet is a technology designed for the control and interaction of real and/or virtual objects over the Internet with minimal latency [12] enabling a tactile experience. This technology not only expands the Internet of Things (IoT) concept, as it introduces an Internet of Virtual Things (IoVT), but also emphasizes the importance of ultra-low latency, high availability, reliability, and enhanced security as its core communication infrastructure attributes [22, 29]. These advancements are crucial for applications that require tactile interaction with objects, such as remote machinery operation or virtual reality, to prevent motion sickness. The integration of 6G, tactile Internet, and advancements in CPI hold transformative potential for participatory healthcare. 6G as the new evolutionary stage of mobile communication technology, characterized by its ultra-reliable low-latency communication (URLLC), is a cornerstone for realizing tactile Internet and enhancing mHealth applications [13]. This technological synergy enables a new dimension of healthcare delivery, where the immediacy of human experiences and cognitive states can be digitally replicated and monitored, facilitating telemedicine and remote surgery with

[1] https://oxalife.com/en-eu/pages/collection
[2] https://www.whoop.com/eu/de/
[3] https://www.empatica.com/en-eu/embraceplus/

unprecedented precision and sensory feedback. Innovative applications leveraging these technologies have been set to revolutionize healthcare delivery. Imagine remote rehabilitation sessions where therapists can not only guide patients through exercises but also feel resistance and movement quality thanks to haptic feedback, while simultaneously monitoring cognitive stress levels to adjust the therapy in real time. Such immersive and interactive experiences can significantly improve treatment adherence and outcomes, heralding a new era of patient-centered and cognitive-informed healthcare [25].

2 SECURITY AND PRIVACY CHALLENGES

The adoption of 6G and the tactile Internet in CPI within healthcare has introduced nuanced security and privacy challenges. As cognitive data are among the most sensitive and personal types of information, safeguarding them is paramount [3, 5]. The complexity of ensuring data protection and compliance with healthcare regulations is heightened when dealing with cognitive data, which may reveal intimate details regarding an individual's mental state, predispositions, and potential health conditions. Wearables can also "read your thoughts" [18] or analyze your inner speech [11] making them extremely intrusive and therefore posing a threat to privacy. Furthermore, the use and distribution of CPI data introduce a variety of threats to privacy, social equality, and health behavior. Medical data from CPI technology have the potential to be used for purposes far beyond analyzing health, fitness, and well-being. One could further argue that cognitive data need to be protected even more thoroughly than medical data currently, for example, by the GDPR [17]. It is yet unclear what can be deduced from cognitive data in the future, and non-democratic states are already using technology to oppress various stakeholders with different technologies [26, 27, 30], which is also known as digital authoritarianism [9, 16].

One possible scenario could be establishing premium systems that reward or penalize individuals based on their health behavior. Such systems could lead to increased insurance costs or reduced benefits for those categorized as leading unhealthy lifestyles or reward individuals that achieve healthy behavior [23]. Permanent surveillance reminds us of the characteristics of a state of surveillance, potentially resulting in different psychological and social effects. While some of the disadvantaged may feel motivated to adopt a healthier lifestyle, others may experience psychological and physical stress, which may lead to an unhealthy lifestyle. In addition, financial rewards can lead to suppression or loss of intrinsic motivation. These rewards can lead to a person not engaging in healthy behavior in the future without financial incentives [33]. These behavioral changes cannot only be related to factors that deal with physical conditions. A few studies have examined real-time monitoring to assess self-injurious thoughts and behavior [19]. Data have been collected using questionnaires and electronic diaries in real time and natural environments [28]. More recently, wearables and smartphone sensors have been used as well. These devices are part of a so-called Wireless Body Area Network (WBAN) [24, 39]. This type of wireless network consists of wearable (e.g., smartwatches) or implanted devices and sensors that collect and transmit physiological data. These developments pave the way for collecting data via human-computer interaction in the future. [19]. The cognitive, personal informatics being collected is highly sensitive and increases the risk of misuse. Measurement errors and inaccuracies in the data could lead to doctors wrongly committing people or suggesting excessive medication. On a positive note, the low latency of 6G means that data can be received in real-time, preventing more severe consequences in an emergency. Several papers already address the growing importance of WBANs for health monitoring [24, 39]. They address the structure, functions, and security challenges of those networks.

In addition to individual impacts, medical data security presents significant risks. Numerous challenges arise in data collection and sharing for research purposes, including increased cyberattacks on databases in hospital systems [37] and transmission networks. In particular, the interconnectivity between medical devices and other systems [35]. Despite anonymization, data traceability and associated re-identification risk cannot be reduced to zero. It can protect the patient's privacy [21]. One of the reasons for this risk may be that certain information necessary for the analysis, such as age and sex, cannot be concealed without harming the usefulness of the research. These developments facilitate the tracing and identification of data sources. However, an approach, the PAX authorization system, combines anonymization with pseudonymization and eXtensible Access Control Markup Language (XACML). This concept ensures security and protection of privacy [1].

The increased attack surfaces and potential vulnerabilities associated with advanced technologies such as 6G and the tactile Internet could lead to unauthorized access to cognitive data, posing significant risks to patient privacy and trust. The real-time nature of 6G-enabled CPI applications further complicates this landscape, as any delay or disruption in security protocols can have immediate and detrimental effects on patient care. Addressing these challenges requires a robust security framework that protects data integrity and confidentiality and ensures the reliability and availability of cognitive informatics services. This necessitates the development of sophisticated threat modeling to anticipate and mitigate potential security threats. For example, a threat model for a cognitive health monitoring system might identify vulnerabilities, such as unauthorized access to cognitive state data, which could lead to privacy breaches or the manipulation of treatment recommendations.

To address all these vulnerabilities, comprehensive security frameworks must be developed that incorporate advanced encryption techniques, secure data storage solutions, and stringent access controls. Moreover, regular security assessments and updates are crucial for adapting to emerging threats in this rapidly evolving technological landscape. Furthermore, the dynamic and highly interconnected nature of 6G networks complicates securing these systems. Traditional security measures may not suffice because of the network's ability to reconfigure rapidly and the introduction of new technologies, such as network slicing, which creates multiple virtual networks on the same physical infrastructure. While these features are beneficial for network efficiency and customization, they introduce new vulnerabilities and complexities to network management and security.

Beyond the risks addressed here, the digital aggregation and analysis of CPI data also offer significant opportunities for research, early detection of diseases, and optimization of patient care. The

constant availability of data enables health insurance companies to proactively encourage customers to seek medical advice, especially if there are signs of serious illness, to ensure timely and appropriate treatment. This approach can significantly improve the quality of medical care through more effective symptom monitoring and optimization of treatment strategies in cooperation with specialists [8]. Especially in rural areas, where access to medical facilities often includes significant effort, digital services, such as video consultations, can play an increasingly important role. Innovations such as the tactile Internet and 6G technology can increase the efficiency and precision of such remote consultations by enabling interactive, immediate communication between patients and doctors that goes beyond video conferencing as we experience it today. This is particularly true in teleneurology and the availability of neurologists [34].

Furthermore, detailed and comprehensive medical data are valuable for further scientific progress. This forms the basis for developing innovative treatment methods and new medicines. Systematic analysis of these data can help assess the relationship between symptoms and diseases. It can also promote an understanding of complex disease patterns and personalized therapeutic approaches adapted to specific patient needs and circumstances.

For these reasons, it is essential to raise awareness on privacy, security, data protection, and surveillance matters. The extensive use of medical data requires careful consideration of the potential benefits to individual and public health and the risks to social justice and individual privacy. An integrated strategy involving data protection measures, legal frameworks, technical safety measures, and initiatives for awareness and education is essential to address upcoming challenges and risks.

3 ETHICAL AND DESIGN CONSIDERATIONS

The deployment of 6G and the tactile Internet into CPI raises critical ethical considerations. The constant and pervasive monitoring of cognitive states creates significant questions about patient privacy, consent, and autonomy, thus ethical design principles become crucial in developing CPI technologies. In particular, integration with artificial intelligence raises challenges and questions about what good patient care can look like and whether there are limits to technology [6].

It remains unclear how privacy should be protected, especially when CPI can analyze inner speech. For example, current consent mechanisms are often not clearly formulated and violate users' rights [32]. If CPI is scaled to mass adoption these consent mechanisms must be clear and not provide legal loopholes for further analysis of cognitive data without explicit permission. For such devices, it must be possible and easy to withdraw consent and be sure that all data is deleted. This is often a challenge at this time [7]. The ability for people to be in control of their own data is also essential for their autonomy, especially in the context of healthcare, for example when patient data is used without their consent [41]. With the advent of 6G, the systems will become real-time and tactile. Therefore, consent must be given before the actual use of CPI and correlating systems as well as for any potential updates of the app. In addition, concepts such as temporal perturbation can be used to protect users' privacy [40].

To prevent unfair treatment conditions, access to CPI technologies must be made available to all users, including those who need assistance due to financial means, age, or condition. This may require financial support or specifically digitally trained staff, which is often a challenge. [20]. It is also important to ensure that health insurance companies and algorithms, such as those used for processing, do not lead to discrimination. Misuse must be prevented. This could be monitored by regular announced and unannounced checks. In addition, the economic interests of health insurance funds and other companies must be subordinated to the interests of the individual. This is another measure to ensure the ethical and equal treatment of all people.

While some of these measures may be difficult to implement, a realistic plan should be in place before CPI technologies are used to permanently retrieve data. These principles should guide how cognitive data are collected, analyzed, and used, ensuring transparency and giving individuals control over their information.

Moreover, the design of CPI technologies must carefully navigate the potential for unintended consequences, such as the exacerbation of health disparities or the stigmatization of certain cognitive states. By involving diverse stakeholders in the design process, including patients, cognitive scientists, ethicists, and technologists, solutions can be crafted that genuinely enhance cognitive well-being without compromising ethical standards or personal autonomy.

4 PROPOSING A RESILIENT FRAMEWORK

Resilience describes the "*ability [of a system] to persist, adapt or transform in the face of change*" [2, 10]. This definition is not limited to technical systems alone but to organizations, communities, and political systems. The conditions for resilient systems are a certain degree of preparation, risk avoidance, and flexible responsiveness. Resilience means using crises as an opportunity. A resilient security framework for 6G-enabled CPI in healthcare must address the unique challenges posed by cognitive data's real-time, sensitive nature. This framework should incorporate advanced encryption techniques, secure data transmission protocols, and dynamic access controls tailored to the high-speed, low-latency requirements of 6G networks. Enhancing system resilience also involves designing for fault tolerance and rapid recovery, ensuring that CPI services remain available and reliable even in the face of cyber incidents, which they will suffer from as other industries did, for example, by Advanced Persistent Threats [31]. Continuous innovation, informed by the latest developments in cybersecurity and cognitive science, is essential to anticipate and counter emerging threats in this field, as both fields are developing quickly. In addition to technical measures to protect medical data, a comprehensive privacy policy should be part of the framework. This includes sensitizing users to data protection and risks. Awareness of potential risks should be increased, and users should learn how to handle their data correctly and conscientiously.

5 DISCUSSION AND RECOMMENDATION

Supporting the secure and ethical implementation of 6G and tactile Internet technologies for CPI in healthcare requires targeted policy initiatives and collaborative efforts. The use cases discussed in this paper show that there are both positive and negative aspects. A

system of rewards and punishments can be used in healthcare to encourage healthy lifestyles and improve adherence to treatment plans. However, there is a risk that such systems can increase inequalities and psychological pressure on patients. Cyberattacks on medical databases pose a severe threat nowadays that not only risks patient privacy but can also disrupt the availability of medical services, leading to severe consequences for patients' care. Therefore, robust security measures are necessary. Digital technologies enable collaboration between specialists across disciplines and geographical boundaries, improving the quality of treatment. 6G and the tactile Internet are transforming medical care by enabling real-time communication for remote examinations and surgeries, which is particularly helpful for people with difficulty accessing medical care. Policymakers and other stakeholders should collaborate to consider specific guidelines and standards for cognitive data protection, addressing the unique vulnerabilities and ethical concerns associated with real-time cognitive monitoring and intervention. Future research should explore the interplay between cognitive state monitoring, user engagement, security, privacy, and technology design. Future CPI interventions must aim for maximum efficacy, resilience, and user satisfaction. As we envision the future landscape of participatory healthcare enabled by these advanced technologies, we define the following four items as crucial to ensure that these technologies are developed in a patient-centric way and maintain security, privacy, and autonomy.

- *Regulatory Adaptation:* Today's health regulations must adapt to rapidly evolving technologies. The challenges and risks posed by 6G and the tactile internet must be addressed to ensure cybersecurity and data protection. Added to this are the dangers of advanced digital health services that invade privacy, e.g., by analyzing inner speech. In addition to integrity and availability, the regulatory adaptation will ensure patients' privacy and data protection rights.
- *Stakeholder Collaboration:* To ensure optimal healthcare and ethical standards, it is essential to foster collaboration between technology developers, healthcare providers, policymakers, and patient representatives. This collaboration enables medical and ethical considerations when developing and using new healthcare technologies. This approach contributes to an ethical and patient-centered healthcare system.
- *Funding and Research:* Further research is essential for using 6G and CPI safely. Therefore, a range of resources must be made available. These include financial resources and access to expertise, technology platforms, and relevant information, for example, from devices such as smartwatches or fitness trackers. Collaboration between different research organizations and regular exchanges are also helpful. This can support the development of safe and ethically acceptable applications.
- *International Standards and Guidelines:* To ensure security and data protection in the CPI sector, developing international regulations and standards is helpful. Cooperation across national and continental borders is essential as the world becomes increasingly interconnected. In addition to protecting privacy and personal data, common standards promote trust in these new technologies. International guidelines broadly view technological progress and individual rights to ensure the safe implementation of 6G, tactile internet, and CPI technology.

ACKNOWLEDGEMENT

The authors gratefully acknowledge funding from the *Federal Ministry of Education and Research* (16KISR001K & 16KISR002 "HealthNet", 16KIS1628K & 16KIS1629 "UbiTrans"), and the *Federal Office for Information Security of Germany* (grants 01MO23033B "5Guide" and 01MO23025B "Pentest-5GSec").

REFERENCES

[1] Al-Zubaidie, M., Zhang, Z., and Zhang, J. Pax: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system. *International Journal of Environmental Research and Public Health 16*, 9 (2019), 1490.

[2] Azadegan, A., and Dooley, K. A typology of supply network resilience strategies: complex collaborations in a complex world. *Journal of Supply Chain Management 57*, 1 (2021), 17–26.

[3] Baumhör, C., Henning, T., and Grosse-Kampmann, M. Threat Modeling Towards Resilience in Smart ICUs. *Communications in Computer and Information Science 1884* (2024). to appear.

[4] Benerradi, J., A. Maior, H., Marinescu, A., Clos, J., and L. Wilson, M. Exploring machine learning approaches for classifying mental workload using fnirs data from hci tasks. In *Proceedings of the Halfway to the Future Symposium 2019* (2019), pp. 1–11.

[5] Cagnazzo, M., Hertlein, M., Holz, T., and Pohlmann, N. Threat modeling for mobile health systems. In *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)* (2018), IEEE, pp. 314–319.

[6] Das, K., Pattanaik, M., Basantia, S., Mishra, R., Das, D., Sahoo, K., and Paital, B. Informatics on a social view and need of ethical interventions for wellbeing via interference of artificial intelligence. *Telematics and Informatics Reports* (2023), 100065.

[7] Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., and Holz, T. We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. *arXiv preprint arXiv:1808.05096* (2018).

[8] Di Cerbo, A., Morales-Medina, J. C., Palmieri, B., and Iannitti, T. Narrative review of telemedicine consultation in medical practice. *Patient preference and adherence* (2015), 65–75.

[9] Dragu, T., and Lupu, Y. Digital authoritarianism and the future of human rights. *International Organization 75*, 4 (2021), 991–1017.

[10] Duchek, S. Organizational resilience: a capability-based conceptualization. *Business research 13*, 1 (2020), 215–246.

[11] Fernyhough, C., and Borghi, A. M. Inner speech as language process and cognitive tool. *Trends in cognitive sciences* (2023).

[12] Fettweis, G. P. The tactile internet: Applications and challenges. *IEEE vehicular technology magazine 9*, 1 (2014), 64–70.

[13] Fettweis, G. P., and Boche, H. 6g: The personal tactile internet—and open questions for information theory. *IEEE BITS the Information Theory Magazine 1*, 1 (2021), 71–82.

[14] Fridman, L., Reimer, B., Mehler, B., and Freeman, W. T. Cognitive load estimation in the wild. In *Proceedings of the 2018 chi conference on human factors in computing systems* (2018), pp. 1–9.

[15] Gomes, N., Pato, M., Lourenço, A. R., and Datia, N. A survey on wearable sensors for mental health monitoring. *Sensors 23*, 3 (2023), 1330.

[16] Huang, J., and Tsai, K. S. Securing authoritarian capitalism in the digital age: The political economy of surveillance in china. *The China Journal 88*, 1 (2022), 2–28.

[17] Ienca, M., and Malgieri, G. Mental data protection and the gdpr. *Journal of Law and the Biosciences 9*, 1 (2022), lsac006.

[18] Kapur, A., Kapur, S., and Maes, P. Alterego: A personalized wearable silent speech interface. In *23rd International conference on intelligent user interfaces* (2018), pp. 43–53.

[19] Kleiman, E. M., and Nock, M. K. Real-time assessment of suicidal thoughts and behaviors. *Current Opinion in Psychology 22* (2018), 33–37.

[20] Kuek, A., and Hakkennes, S. Healthcare staff digital literacy levels and their attitudes towards information systems. *Health informatics journal 26*, 1 (2020), 592–612.

[21] Langarizadeh, M., Orooji, A., Sheikhtaheri, A., and Hayn, D. Effectiveness of anonymization methods in preserving patients' privacy: A systematic literature

review. *eHealth 248* (2018), 80–87.

[22] Maier, M., Chowdhury, M., Rimal, B. P., and Van, D. P. The Tactile Internet: Vision, Recent Progress, and Open Challenges. *IEEE Communications Magazine 54*, 5 (2016), 138–145.

[23] Marteau, T. M., Ashcroft, R. E., and Oliver, A. Using financial incentives to achieve healthy behaviour. *Bmj 338* (2009).

[24] Monton, E., Hernandez, J. F., Blasco, J. M., Hervé, T., Micallef, J., Grech, I., Brincat, A., and Traver, V. Body area network for wireless patient monitoring. *IET communications 2*, 2 (2008), 215–222.

[25] Padhi, P. K., and Charrua-Santos, F. 6g enabled tactile internet and cognitive internet of healthcare everything: Towards a theoretical framework. *Applied System Innovation 4*, 3 (2021), 66.

[26] Polyakova, A., and Meserole, C. Exporting digital authoritarianism: The russian and chinese models. *Policy Brief, Democracy and Disorder Series* (2019), 1–22.

[27] Qiang, X. President xi's surveillance state. *J. Democracy 30* (2019), 53.

[28] Shiffman, S., Stone, A. A., and Hufford, M. R. Ecological momentary assessment. *Annu. Rev. Clin. Psychol. 4* (2008), 1–32.

[29] Simsek, M., Aijaz, A., Dohler, M., Sachs, J., and Fettweis, G. 5g-enabled tactile internet. *IEEE Journal on selected areas in communications 34*, 3 (2016), 460–473.

[30] Tian, X. An interactional space of permanent observability: Wechat and reinforcing the power hierarchy in chinese workplaces. In *Sociological Forum* (2021), vol. 36, Wiley Online Library, pp. 51–69.

[31] Urban, T., Grosse-Kampmann, M., Tatang, D., Holz, T., and Pohlmann, N. Plenty of phish in the sea: Analyzing potential pre-attack surfaces. In *Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part II 25* (2020), Springer, pp. 272–291.

[32] Urban, T., Tatang, D., Degeling, M., Holz, T., and Pohlmann, N. Measuring the impact of the gdpr on data sharing in ad networks. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security* (2020), pp. 222–235.

[33] Vlaev, I., King, D., Darzi, A., and Dolan, P. Changing health behaviors using financial incentives: a review from behavioral economics. *BMC public health 19*, 1 (2019), 1–9.

[34] Wechsler, L. R. Advantages and limitations of teleneurology. *JAMA neurology 72*, 3 (2015), 349–354.

[35] Williams, P. A., and Woodward, A. J. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research* (2015), 305–316.

[36] Wilton, A. R., Sheffield, K., Wilkes, Q., Chesak, S., Pacyna, J., Sharp, R., Croarkin, P. E., Chauhan, M., Dyrbye, L. N., Bobo, W. V., et al. The burnout prediction using wearable and artificial intelligence (brownie) study: a decentralized digital health protocol to predict burnout in registered nurses. *BMC nursing 23*, 1 (2024), 1–14.

[37] Wright, A., Aaron, S., and Bates, D. W. The big phish: cyberattacks against us healthcare systems. *Journal of General Internal Medicine 31* (2016).

[38] Xu, Y., De la Paz, E., Paul, A., Mahato, K., Sempionatto, J. R., Tostado, N., Lee, M., Hota, G., Lin, M., Uppal, A., et al. In-ear integrated sensor array for the continuous monitoring of brain activity and of lactate in sweat. *Nature Biomedical Engineering 7*, 10 (2023), 1307–1320.

[39] Yaghoubi, M., Ahmed, K., and Miao, Y. Wireless body area network (wban): a survey on architecture, technologies, energy consumption, and security challenges. *Journal of Sensor and Actuator Networks 11*, 4 (2022), 67.

[40] Yang, X., Ren, X., Yang, S., and McCann, J. A novel temporal perturbation based privacy-preserving scheme for real-time monitoring systems. *Computer Networks 88* (2015), 72–88.

[41] Zhang, H., Zhang, H., Zhang, Z., and Wang, Y. Patient privacy and autonomy: a comparative analysis of cases of ethical dilemmas in china and the united states. *BMC Medical Ethics 22*, 1 (2021), 1–8.