LEGAL AND ETHICAL IMPLICATIONS OF WEARABLE HEALTH TECHNOLOGIES: A COMPARATIVE ANALYSIS OF PRIVACY, LIABILITY AND CONSENT IN INDIA, EU AND THE UNITED STATES

Khushee Sabharwal, LLB, Symbiosis Law School, Pune

ABSTRACT

Wearable health technologies, including smartwatches, fitness trackers, continuous glucose monitors, and AI-powered health applications or 'health apps', are powering change in how healthcare is delivered by enabling real time monitoring, targeted interventions, and early diagnosis. However, these technologies collect continuous and highly sensitive health data, which creates real issues in terms of privacy, consent, data governance, cross-border transfers, and liability. This paper will critically consider these issues primarily through the lens of Indian constitutional jurisprudence, particularly the right to privacy established in Justice K.S. Puttaswamy v. Union of India, and statutory developments under the Digital Personal Data Protection Act, 2023 (DPDP Act) and India's Medical Device Rules, 2017. In addition, it will reflect on inequalities in access to wearable devices, the ambiguity around who is liable for incorrect readings, consumer protection, medical negligence, judicial principles, and statutory developments in these areas. A comparative framework will consider the EU's regulatory framework under the General Data Protection Regulation or GDPR and sectoral laws in the United States such as HIPAA and CCPA. This paper identifies areas of tension in the law, including the limits of anonymisation, opaque algorithms, dual-use dilemma, and discrimination risk while identifying burgeoning regulatory trends across jurisdictions. Lastly, this paper will present regulatory reforms in policy advocating for further investments in privacy; by-design, crisp consent standards, accountability for meaningful algorithmic transparency, coherent regulatory oversight, and robust data-governance models.

Keywords: Wearable Health Technology, Privacy, Consent, Liability and Data Protection

INTRODUCTION

Wearable health technologies; smartwatches, fitness trackers, continuous glucose monitors, smart watches and allied digital tools (mobile health apps, telemedicine platforms, AI diagnostics) are reshaping healthcare delivery. They promise better prevention, earlier diagnosis, remote monitoring and personalised interventions. But they also generate continuous, granular, and highly sensitive health data: heart rhythms, sleep patterns, menstrual cycles, location-linked activity, and sometimes raw biometric signals. This raises complex legal questions about privacy, data governance, consent, liability, and the appropriate regulatory framework. This critical analysis examines these issues through the provisions of constitution and legislations on data privacy. It identifies core legal tensions, practical challenges, and recent policy developments that shape how law and regulation should treat wearable health data.

ANALYSIS

Consent is integral to privacy and with the coming of an age of health wearables it has become increasingly a concern. It is usually in the form of a check box that appears at the end of a lengthy notice that pops up as soon as a user visits a website or an app. This is the reason by which we as users unknowingly and unintentionally consent to unauthorised use of our personal information. In the case of wearables there is no such system and the consent is passive, i.e without the user realizing it. For health data, legal regimes often require explicit consent and a granular, revocable mechanism. Courts and regulators are increasingly sceptical of bundled or opaque consent, especially where user comprehension is doubtful. Legal frameworks therefore push for stronger governance, purpose limitation, strict minimisation, and default privacy-protective settings, rather than relying purely on repeated explicit consent as a panacea.

PRIVACY AS A FUNDAMENTAL RIGHT

The advent of technology has given a substantial boost to the health industry. There are a plethora of wearables or devices including smart watch, which can be worn on hand, wrist or as a ring on a finger etc, to track heart rate, blood pressure and other imperative parameters. The problem stems with the invasion of data privacy as there is no manner by which a potential user can consent to the information that such devices collect or even if there is unauthorised sharing of such sensitive personal information. In India, for example, the Supreme Court's

landmark decision in *Justice K.S. Puttaswamy Vs Union of India*[1] affirmed privacy as a fundamental right under *Article 21*[2], of the constitution of India. This judgment is frequently invoked when assessing state or private intrusions into health-related data flows.

In addition websites and health applications constitute another huge area that not only lack a consent mechanism as stated above but also a legislative framework to be governed by and decide liability in cases of breach. One possible solution is found in *Shreya Singhal Vs Union of India*[3] which upheld an online intermediary's responsibility to remove the content when intimated through a government order. Therefore governments can choose to regulate data of its citizens by overseeing the functioning of such health websites and applications. In *Selvi Vs State of Karnataka*[4], the Supreme Court held that forcibly conducting narco-analysis and brain-mapping without consent was a violation of privacy and consent was essential for the same.

UNEQUAL ACCESS TO SUCH HIGH END DEVICES

The wearable devices can also ensure prediction of a disease by guiding the consumer accurately as the approach is personalised and thus it can enhance health equity by taking a step towards making health services digital. One problem to this is the unequal access to such high end devices and websites. This is because the use of these websites and devices is confined to resourceful and digitally literate services. This can even lead to bias in prediction of diseases if incorporated in a survey as the underprivileged sections are the most vulnerable to major health diseases owing to lack of education, awareness, sanitation and hygiene. This is in turn a violation of *Article 14*[5] and *Article 15*[6] of the constitution of India. In *Consumer Education and research Centre Vs Union of India*[7], it was stressed upon that depriving workers engaged in hazardous industries of sufficient medical healthcare would be discriminatory. In *State of Punjab Vs Ram Lubhaya Bagga*[8] the role of governments to not formulate health policies that disproportionately disadvantage certain groups was affirmed.

[1] Justice K.S. Puttaswamy Vs Union of India, 2019 (1) SCC 1
[2] INDIA CONST. art. 21
[3] Shreya Singhal vs U.O.I, 2015 (2) SCC (CRI) 449
[4] Selvi Vs State of Karnataka, (2010) 7 S.C.C. 263
[5] INDIA CONST. art. 14
[6] INDIA CONST. art. 15
[7] Consumer Education and Research Centre v. Union of India, (1995) 3 SCC 42
[8] State of Punjab v. Ram Lubhaya Bagga, (1998) 4 SCC 117

DETERMINATION OF LIABILITY IN CASES OF INACCURATE READINGS ON MEDICAL DEVICES OR WEARABLES

The central question to this discussion is the determination of liability for inaccurate readings on medical devices. In *Indian Medical Association Vs V.P. Shantha*[9], Supreme court stated that medical services could fall under the ambit of consumer protection by allowing the patients remedies due to negligence stemming from faulty medical instruments. In *Kunal Saha Vs Dr Sukumar Mukherjee*[10], the apex court provided high compensation for medical negligence highlighting that breach in the duty of care, including belief in defective medical tools amounted to liability. Medical wearables can are now considered as medical devices under *Medical Device Rules,2017*[11] if they make any claim with regard to diagnosis or therapeutic value of the same. In addition, according to the *Consumer Protection Act,2019*[12] patients and consumers may bring about product liability suits against manufacturers and service providers when inaccurate readings lead to harm. In *Medtronic, Inc. v. Lohr* [13](1996) the Supreme Court of United States allowed state tort claims for defective medical devices despite federal regulation, and in *A v. National Blood Authority*[14], (2001)(U.K.), the court imposed strict liability under product liability law for supplying defective health products.

EXISTING LEGISLATIONS GOVERNING DATA PRIVACY : A COMPARATIVE PERPSECTIVE BETWEEN INDIAN AND INTERNATIONAL JURISPRUDENCE

CHARACTERISTIC OF COMPARISON	INDIA	EUROPEAN UNION	UNITED STATES OF AMERICA
MAIN LEGISLATION AND CONSTITUTIONAL BASIS	Right to Privacy; Article 21, K. Puttaswamy case, Digital Personal Data Protection Act, 2023	Charter of Fundamental Rights(Article 7 and 8), General Protection Data Regulations, 2016	Privacy right a part of sectoral laws Health Insurance Portability and Accountability Act,1996(HIPAA); Federal Trade Commission(FTC), California Consumer

[9] Indian Medical Association v. V.P. Shantha, (1995) 6 S.C.C. 651
[10] *Kunal Saha v. Dr. Sukumar Mukherjee*, (2014) 1 S.C.C. 384
[11] Medical Device Rules, 2017 (2017) India
[12] Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).
[13] Medtronic, Inc. v. Lohr, 518 U.S. 470 (1996)
[14] A v. National Blood Authority, [2001] 3 All E.R. 289 (Q.B.)

			Privacy Act,2018(CCPA)
CATEGORIZATION OF HEALTH DATA	Sensitive personal data(includes health wearables)	Data under Article 9 GDPR.	Covered under HIPAA for medical entities, consumer apps largely unregulated
CONSENT	Explicit, informed, revocable, confined to purpose	Explicit, informed, additional safeguards for automated processing	Authorisation required for sharing medical information, FTC is a regulation against unfair trade practices
CROSS BORDER DATA TRANSFER	Conditional, fiduciary accountability, sufficient safeguards	Strict regulation	Minimal federal restriction
LEGISLATIVE AUTHORITY	Data Protection Board, Sectoral regulators for medical devices	Data Protection Authority across the EU, EU court of justice the supervisory authority	Office for civil rights(HIPAA), state attorneys for CCPA
PENALTY	Fines upto Rs 5 Crores	< 20 million	Civil penalties and state fines under CCPA
CONSEQUENCES FOR WEARABLES	Mandatory compliance with DPDP Act, 2023 and Medical Device rules,2017	GDPR governs processing; explicit consent, purpose, limitation, strict accountability	HIPAA for medical entities, FTC for unfair trade practices.

CHALLENGES

1. Continuous, high-granularity data and identifiability

Wearable data is high-frequency and can be highly revealing (patterns of movement, sleep, physiological responses). Even when "unidentified" combining multiple streams can re-identify individuals or reveal sensitive conditions. Legal tests for effective anonymisation are

hard to satisfy in practice and raise questions about the adequacy of current anonymisation standards.

2. Cross-border transfers and cloud ecosystems

Wearable data is often stored and processed in global clouds. Cross-border transfer rules (data localization or adequacy regimes) complicate compliance which in turn makes deciding the jurisdiction even more difficult. Data fiduciaries must map transfers, understand local data export rules, and ensure contractual and technical safeguards.

3. Informational asymmetry and opaque algorithms

Artificial Intelligence and Machine Learning models trained on wearable data often operate as black boxes. Usually the users cannot effectively inspect algorithmic inferences that affect medical advice or insurance decisions. This opacity undermines informed consent and complicates regulators' ability to assess fairness, bias, and safety.

4. Dual-use tension: clinical utility vs. commercial exploitation

There's a tension between legitimate secondary uses (research, population health) and commercial exploitation (targeted advertising, behavioural nudging). Legal regimes must balance enabling beneficial uses (with safeguards) against exploitation. Consent for research must be robust, and governance structures (ethics boards, data trusts) may be needed to legitimise secondary uses.

5. Employment and insurance contexts

Mandated wearables in workplaces or insurer-provided devices can create coercive contexts for consent and risk discriminatory decisions (fitness-for-work, pregnancy inference). Anti-discrimination laws and data protection principles must be harmonised to prevent misuse.

RECENT DEVELOPMENTS

Several policy and enforcement developments illustrate evolving regulatory pressure:

1. Constitutional and statutory recognition of privacy as a legal right and the rise of comprehensive data-protection statutes have created enforceable duties for data

processors handling health data; in India, the DPDP Act are shaping how health data must be processed, with obligations on notice, consent and data fiduciaries.

2. In the EU, GDPR continues to treat health data as a special category that demands heightened protections and specific lawful bases for processing, influencing global practices and contractual terms for cross-border data flows.

3. Regulators have clarified the boundary for medical-device oversight: agencies like the FDA focus regulatory resources on software functions that present greater risk to patients and have issued guidance to help developers classify their products and meet obligations (or assert non-enforcement where appropriate). This helps developers but also creates compliance requirements for higher-risk functions.

4. Enforcement actions signal concrete consequences: regulatory settlements and penalties for improper sharing of sensitive health data (notably actions against therapy apps and health-tech firms) and penalties for product safety reporting failures indicate that both privacy and safety dimensions are being policed. These cases have increased industry attention to privacy-by-design, truthful marketing, and robust incident reporting.

5. Workplace and discrimination scrutiny is rising: agencies (e.g., the U.S. EEOC) have warned about potential illegal discrimination arising from misuse of biometric and health metrics collected via wearables, prompting employers to reassess monitoring programs and privacy protections.

LEGAL & POLICY RECOMMENDATIONS

1. **Privacy-by-design and default:** Manufacturers and platform operators should bake minimisation, local processing, and strong default privacy settings into product design. Default opt-outs and minimal data capture should be the norm.

2. **Crisp consent mechanisms:** Consent mechanisms must be short, specific, and contextual ;especially when data is collected passively. For continuous data streams, firms should combine initial explicit consent with ongoing transparency dashboards and easy revocation.

3. **Data governance frameworks:** Entities processing health data should adopt governance (data-protection officers, ethics committees, DPIAs/data protection impact assessments) and contractual controls with processors and cloud providers, mapping cross-border flows and defining permitted secondary uses.

4. **Algorithmic transparency and auditability:** Where decisions based on wearable data have legal/clinical consequences, entities should document models, conduct bias and accuracy audits, and provide meaningful explanations to affected individuals.

5. **Sectoral coordination:** Regulators should coordinate across privacy, medical devices, consumer protection, and labour law spheres to provide clear, harmonised guidance addressing overlap and preventing regulatory gaps.

CONCLUSION

Data privacy in health information is essential. Wearables whether actively or passively not only collect sensitive information about users but also lead them to draw big conclusions about the state of their health. In India right to privacy was established as a fundamental right which further led to the enactment of Digital Personal Data Protection Act,2023 and the regulatory framework under the Medical Device Rules, 2017. These reforms collectively reflect an evolving recognition of the urgent need to safeguard sensitive health information in the digital era. between these two approaches, faces the pressing task of not only operationalising its new data protection regime but also clarifying liability for defective digital health devices under the Consumer Protection Act, 2019 and principles of tort law. Lastly, the credibility of digital health innovation rests on public trust. This can be achieved only by striking a balance between promoting technological progress and ensuring accountability through stringent consent mechanisms, well-defined liability standards, and transparent governance of health data. As the judiciary and legislature continue to adapt to the demands of the digital age, the future of wearable health technologies will rely not merely on technical sophistication but also on the development of a legal ecosystem that guarantees patient safety, individual autonomy, and human dignity.