The Digital Pulse

Health Sensors and the Privacy Dilemma

Benedetta Burston
SDA Bocconi School of Management

European Health Data Space – Secondary Use of Data and Data Subject Rights
Individuals and Fundamental Rights in the EHDS

Presentation Overview

Part I - Problem Framing

1. **Research Framework & RQs**
2. **Context: Wearable Health Technologies**
3. **Technical Vulnerabilities**
4. **Stakes of the Problem**

Part II - Regulatory Analysis

5. **Consent Analysis**
6. **EU Regulatory Framework (GDPR / EHDS)**
7. **US Regulatory Framework (HIPAA / FTC)**
8. **Comparative Analysis**

Part III - Synthesis & Recommendations

9. **Central Argument**
10. **Discussion**
11. **Privacy by Design**
12. **Policy Recommendations**

Analytical Framework and Research Questions

Theoretical Grounding

Contextual Integrity (Nissenbaum, 2004; Gilbert, 2024)

Information flows appropriately only when they match the norms of the original context. Wearable data crosses from consumer/wellness into healthcare governance = a structural mismatch.

Surveillance Capitalism (Zuboff, 2019)

Continuous behavioural data extraction as a logic of capital accumulation. EHDS secondary use risks institutionalising this logic within public governance frameworks.

Data Governance (Lianos et al., 2025; DeNardis 2020)

Governance of data as infrastructure requires ex ante design constraints, not only ex post liability, a principle wearable health data directly tests.

Research Questions

RQ1

How does the continuous, passive, and context-crossing nature of wearable health data undermine the conditions for valid consent under EU data protection law?

RQ2

How does the EHDS secondary use regime amplify these consent deficits at scale?

RQ3

How do the EU and US regulatory models compare in their structural capacity to govern downstream reuse of wearable-generated health data?

Analytical Framework and Research Questions

Theoretical Grounding

Contextual Integrity (Nissenbaum, 2004; Gilbert, 2024)

Information flows appropriately only when they match the norms of the original context. Wearable data crosses from consumer/wellness into healthcare governance = a structural mismatch.

Surveillance Capitalism (Zuboff, 2019)

Continuous behavioural data extraction as a logic of capital accumulation. EHDS secondary use risks institutionalising this logic within public governance frameworks.

Data Governance (Lianos et al., 2025; DeNardis 2020)

Governance of data as infrastructure requires ex ante design constraints, not only ex post liability, a principle wearable health data directly tests.

Research Questions

RQ1

How does the continuous, passive, and context-crossing nature of wearable health data undermine the conditions for valid consent under EU data protection law?

RQ2

How does the EHDS secondary use regime amplify these consent deficits at scale?

RQ3

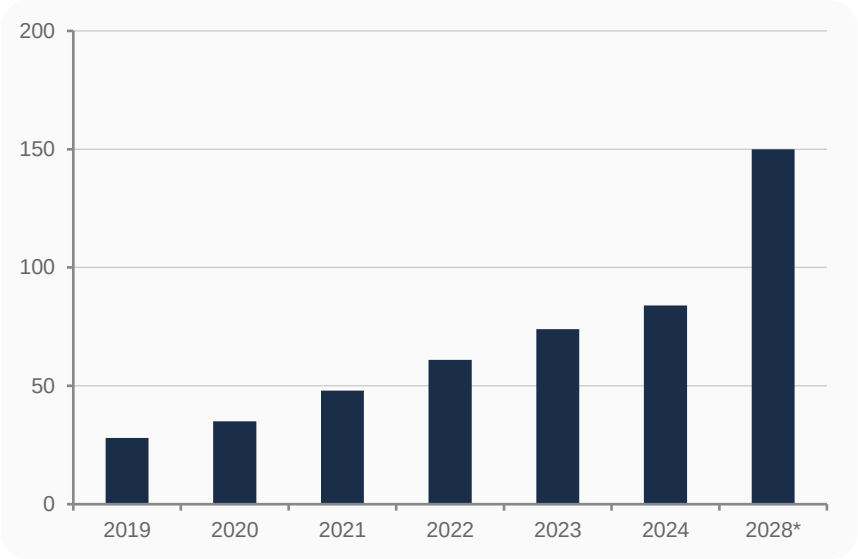
How do the EU and US regulatory models compare in their structural capacity to govern downstream reuse of wearable-generated health data?

Wearable Health Technologies: scope and market scale

Data Categories x Regulatory Status

Category	Data Types	EHDS Secondary Use Status
Biometric	Heart rate, SpO2, ECG, galvanic response	Grey zone; eligible for EHDS secondary use as “health data” when aggregated
Metabolic (CGM)	Blood glucose, caloric expenditure	Special category (Art. 9 GDPR); EHDS secondary use requires explicit legal basis
Behavioural	Sleep, movement, location cycles	Largely unregulated; re-identification risk in EHDS data spaces via aggregation
Reproductive	Menstrual cycles, fertility, temperature	Special category (contested); secondary use via EHDS altruism frameworks unresolved
Neurological	EEG, cognitive patterns, stress indicators	Minimal regulatory coverage; no EHDS secondary use framework yet established

Global Wearable Technology Market (USD Billion)



** Forecast. Sources: Grand View Research; Fortune Business Insights; MarketsandMarkets (2025)*

Technical vulnerabilities in wearable data transmission

Wearable sensors transmit data via APIs, Wi-Fi, and Bluetooth to third-party apps and cloud platforms. Fragmented API ecosystems and BLE attack surfaces - combined with inadequate regulatory oversight - create a structural privacy deficit.

APIs & Data Transmission

Wearable sensors transmit via APIs to third-party apps or cloud storage. Gartner's Market Guide for API Protection (2024) identifies APIs as the leading cause of data breaches.

Gartner (2024)

BLE Vulnerabilities

BLE has known vulnerabilities exposing data to eavesdropping and hijacking attacks. BLESA allows attackers to bypass authentication and intercept live data in transit.

Wu, Nan, Kumar et al. (2020)

OWASP Top API Security Risks (2019)

1. Broken object-level authorization
2. Broken user authentication
3. Excessive data exposure
4. Lack of resources & rate limiting
5. Function-level auth failure
6. Security misconfiguration (+ 3 more)

OWASP (2019)

Data Categories Transmitted

Heart rate, sleep, GPS, blood oxygen, reproductive health, glucose levels. Together these form a comprehensive biometric profile far exceeding what users anticipate at consent.

Misuse Pathways

Data forwarded to advertisers, insurers, and employers. De-identified datasets re-identified via cross-referencing. These misuse vectors are compounded by EHDS secondary use pipelines, which institutionalise large-scale data aggregation with derogations that bypass original consent context.

Stakes for Data Subjects under EHDS Secondary Use

When wearable health data is repurposed under EHDS secondary use frameworks, data subjects lose meaningful control over how their most sensitive information is used. The harms are not hypothetical: discrimination, erosion of trust, economic loss, and compromised care are concrete consequences of inadequate data subject rights protections.*Arts. 17, 21, 22 GDPR; EHDS Regulation (2022)*

Risk of Discrimination

EHDS secondary use enables health data to reach employers and insurers via research pipelines. Wearable-derived biometric profiles - including reproductive, metabolic, and neurological data - create new discrimination vectors that opt-out mechanisms alone cannot adequately address.

Loss of Trust

If data subjects cannot meaningfully exercise rights of access, erasure, or objection (Arts. 15–21 GDPR) once data enters EHDS data spaces, trust in both healthcare institutions and the regulatory framework itself is undermined - reducing participation in digital health programmes.

Economic Harm

Inadequate data subject rights protections expose EHDS-participating institutions to significant liability. GDPR fines reached EUR 1.78B in 2023; EHDS non-compliance could trigger enforcement at scale given the volume and sensitivity of data spaces involved.

DLA Piper (2025); GDPR Enforcement Tracker

Compromised Healthcare

If patients cannot trust that wearable data will not be reused beyond its original clinical context, they will withhold information from physicians - directly degrading data quality within the very EHDS health data spaces designed to improve EU public health outcomes.

The structural inadequacy of consent models

GDPR Art. 4(11) / Recital 32: *Consent must be "freely given, specific, informed, and unambiguous." Art. 9 imposes heightened requirements for health data as a special category.*

A. Consent at Registration

One-time consent obtained at device setup cannot logically cover data uses not yet specified. This conflicts with the specificity requirement (Recital 33) and the purpose limitation principle (Art. 5(1)(b)).

Art. 5(1)(b) GDPR; Solove (2013)

B. Implied and Bundled Consent

Connecting third-party apps via SSO/SAML constitutes at most implied consent. Blanket consent frameworks do not satisfy the unambiguous standard. FTC v. Flo Health (2021) illustrates the enforcement gap downstream.

Recital 32 GDPR; FTC v. Flo Health (2021)

C. The Re-identification Problem

HIPAA (45 CFR s.164.514) and GDPR permit secondary use of de-identified data, but de-identification is empirically reversible when datasets are merged. EHDS-scale aggregation structurally intensifies this risk.

Ohm (2010); Sweeney (2002)

GDPR and EHDS

GDPR Framework

Special Category Designation (Art. 9)

Health data requires explicit consent and heightened protection. Wearable-generated wellness data often falls outside the statutory definition, creating an asymmetry within the same device ecosystem.

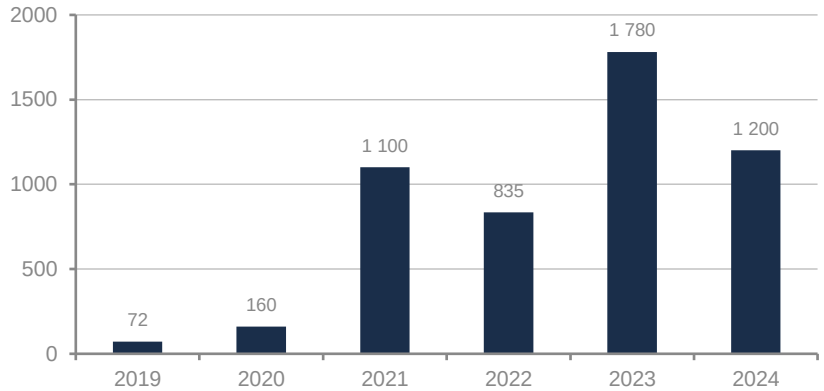
EHDS and Secondary Use

Regulation (EU) 2022/868 and the EHDS establish a framework for secondary use for public interest research. The secondary use logic structurally decouples data reuse from the original consent context.

Cross-Border Complexity

GDPR applies to any entity processing EU citizens' data. The post-Schrems II environment further complicates transatlantic flows for wearable companies operating globally.

GDPR Enforcement: Total Fines by Year (EUR Millions)



Source: DLA Piper GDPR Fines and Data Breach Survey (Jan. 2025); GDPR Enforcement Tracker (CMS Law)

HIPAA and the FTC

HIPAA (1996)

Covered entity limitation

45 CFR s.160.103 restricts HIPAA to healthcare providers, insurers, and business associates. Consumer wearable manufacturers and third-party app developers are structurally outside this scope.

Context-dependent application

The same device data may attract HIPAA protection in a clinical deployment but none in consumer use -an incoherence the statute does not resolve.

De-identification loophole

s.164.514 permits secondary use of de-identified data without consent. When combined with other datasets, such data is empirically reversible (Ohm, 2010; Sweeney, 2002).

FTC Section 5 Enforcement

Ex post consumer protection

Section 5 FTC Act prohibits unfair or deceptive acts. This is the primary federal mechanism for wearable data misuse -but it operates reactively, after harm has materialised.

Enforcement precedents

FTC v. Flo Health (2021): reproductive health data shared with third-party analytics despite privacy representations. Drizly/Rellas (2022): first case of personal CEO liability for data security failures.

Structural limitation

No general federal privacy statute. The patchwork of state regimes (CCPA) and voluntary standards cannot substitute for ex ante structural protections.

Structural comparison

Dimension	European Union	United States
Regulatory model	Ex ante, rights-based (GDPR Arts. 7, 9)	Ex post, enforcement-based (FTC Act s.5)
Legal basis for health data	Special category; explicit consent (Art. 9)	Sectoral (HIPAA); consumer protection
Scope	All controllers processing EU subjects' data	Covered entities only (45 CFR s.160.103)
Secondary use regime	EHDS enables at scale; consent derogations permissible	No federal secondary use framework
Wearable coverage	Partial - consumer wellness data in grey zone	Largely excluded from HIPAA scope
Enforcement	DPAs; fines up to 4% of global turnover (EUR 5.88B cumulative to 2025)	FTC settlements; limited structural deterrence

Shared structural failure: both systems lack adequate ex ante protections for downstream secondary use of continuously generated wearable health data.

Structural tensions in data governance

Central argument: The EHDS does not merely inherit the consent deficits produced by wearable data collection -it structurally amplifies them by institutionalising secondary use at scale, decoupling governance from the original collection context, and legitimising data reuse without adequate rights-based safeguards for always-on biometric data.

1. Innovation vs. Rights

EHDS governance is premised on data as a common resource for public benefit. This logic is structurally in tension with data subject rights grounded in individual autonomy (Westin, 1967; Solove, 2013). The regulation resolves this tension in favour of innovation via derogations and opt-out mechanisms that are inadequate for passively generated biometric data.

Mittelstadt et al. (2016)

2. Scale vs. Specificity

Consent is a mechanism designed for discrete, bounded transactions. Always-on wearables produce data streams that are unbounded in time and scope. The aggregation problem (Solove, 2006) is not incidental but structural: EHDS data spaces are designed to aggregate, not to isolate.

Solove (2006); Nissenbaum (2010)

3. Accountability vs. Traceability

Once health data enters the EHDS secondary use ecosystem, chain-of-custody accountability breaks down. The GDPR accountability principle (Art. 5(2)) becomes formally satisfied but substantively hollow when data controllers can no longer trace how originally consented data has been repurposed.

Art. 5(2) GDPR; Doshi-Velez et al. (2017)

Reassessing data subject rights in always-on environments

D1 The consent model is structurally inadequate

GDPR's consent framework cannot govern data continuously generated by always-on devices. EHDS governance must develop alternative legal bases that provide substantive, not merely formal, protection.

D2 The EHDS amplifies rather than resolves these tensions

By institutionalising secondary use at scale through data spaces and altruism frameworks, EHDS structurally decouples data governance from the rights of original data subjects. Wearable-specific provisions are required within the regulation.

D3 The US sectoral model leaves a larger structural gap

The HIPAA/FTC patchwork leaves most wearable-generated health data without adequate ex ante protection. The absence of a federal privacy statute creates enforcement asymmetries that distort the transatlantic compliance landscape.

D4 Transatlantic alignment is a governance priority

Cross-border data flows require mutual recognition of standards for wearable health data. Post-Schrems II, the lack of an adequate transatlantic framework for this data class constitutes a structural risk to rights operationalisation under both regimes.

Technical Measures as a Necessary Complement to Policy

PRIVACY BY DESIGN

Differential Privacy

Implements Art. 25 GDPR's data minimisation requirement at the technical layer: statistical noise prevents individual re-identification while preserving aggregate utility for secondary research under EHDS.

Homomorphic Encryption

Enables third-party analytics on encrypted wearable data without decryption, giving technical substance to purpose limitation (Art. 5(1)(b) GDPR) beyond contractual assurances alone.

Federated Learning

Models are trained on-device without raw data ever leaving the wearable, structurally preventing the aggregation problem (Solove, 2006) that EHDS data spaces institutionalise.

DATA MINIMIZATION & DECENTRALIZATION

Blockchain

Smart contracts can encode granular consent conditions and enforce chain-of-custody accountability, addressing the traceability breakdown identified under Art. 5(2) GDPR in EHDS ecosystems.

Decentralized Identity Systems

Self-sovereign identity gives data subjects technical control over access without relying on central authorities, operationalising contextual integrity (Nissenbaum, 2004) at the infrastructure level.

Data Minimization

Technical enforcement of collection limits at the device firmware level, not just contractual. Prevents the biometric profile aggregation that renders consent structurally inadequate under EHDS secondary use logic.

Policy Recommendations

1. Wearable-Specific Provisions within EHDS

Amend EHDS to include explicit provisions for always-on biometric wearable data: tiered consent requirements, purpose-specific access controls in data spaces, and mandatory data subject notification when secondary use is authorised.

2. Reinforce Data Subject Rights in Secondary Use

Ensure Arts. 17-21 GDPR rights (erasure, objection, restriction) remain fully operational once data enters EHDS data spaces. Opt-out mechanisms must be technically enforceable, not merely contractual, for wearable-generated data. *GDPR Arts. 17–21; cf. Solove (2013); Westin (1967)*

3. Mandatory Privacy by Design for EHDS Access

Condition EHDS data space access on demonstrated adoption of privacy-preserving technologies (federated learning, differential privacy, homomorphic encryption). Art. 25 GDPR by-design obligations must be technically verified, not self-certified. *GDPR Art. 25; Emami-Naeini et al. (2020)*

4. Transatlantic Alignment on Wearable Health Data

Mutual recognition framework for wearable health data standards between EU and US. Post-Schrems II, EHDS cross-border flows require an adequate transatlantic mechanism; absence creates a compliance asymmetry that distorts both enforcement and innovation incentives. *Schrems II (C-311/18)*

5. Strengthen EHDS Governance & Accountability

Establish independent chain-of-custody audit requirements for wearable data entering EHDS pipelines. Escalating fines for secondary use violations; DPA oversight of data space operators; private right of action for data subjects whose rights are materially compromised by EHDS reuse. *GDPR Art. 5(2);*

Thank you!

LET'S CONNECT

Benedetta.burston@sdabocconi.it

linkedin.com/in/benedetta-burston