

Data Privacy, Ownership, and Secondary Use of Clinical Data Generated by Continuous Glucose Monitors and Mobile Health Applications: A Review

Journal of Diabetes Science and Technology

1–8

© 2026 Diabetes Technology Society



Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/19322968261455365

journals.sagepub.com/home/dstPaulo Dario, PhD¹

Abstract

The growing use of continuous glucose monitors (CGMs) and mobile health (mHealth) applications has changed how diabetes is managed, allowing real-time tracking of glycemic patterns and remote clinical decision-making. These technologies also generate large volumes of sensitive health data, raising questions about who owns this information, how it is protected, and under what conditions it may be repurposed for research or commercial objectives. This review examines the regulatory frameworks governing CGM and mHealth data in major jurisdictions, with particular attention to the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. Significant regulatory gaps exist, particularly for consumer-grade devices and direct-to-consumer mHealth applications that fall outside traditional healthcare data-protection frameworks. Data ownership remains legally ambiguous in most jurisdictions, with patients, healthcare providers, device manufacturers, and app developers each holding competing claims. The secondary use of clinical data for research, while it could materially advance diabetes care, raises ethical concerns around informed consent, data de-identification, and the boundaries between clinical care and commercial exploitation. Emerging approaches, including the European Health Data Space, federated learning, and differential privacy, may help balance data utility with individual rights. The review recommends changes to regulation, industry practice, and consent models aimed at reconciling data-driven diabetes research with patient autonomy and privacy.

Keywords

continuous glucose monitoring, data ownership, data privacy, mHealth, regulatory frameworks, secondary use

Introduction

Continuous glucose monitors (CGMs) sample interstitial glucose every 1–5 minutes, generating up to 1440 readings per day.¹ Integrated with mobile health (mHealth) applications, insulin pumps, and cloud analytics, they produce a continuous stream that also captures activity, diet, medication, sleep, and geolocation.^{2,3} Time in range and the ambulatory glucose profile are now consensus elements of diabetes care.^{4,5} Recent Food and Drug Administration (FDA) clearance of over-the-counter CGMs,⁶ in a market projected to exceed USD 49 billion by 2033,⁷ indicates adoption beyond clinically diagnosed users.

Yet this same granularity reveals information far beyond glucose. A CGM trace shows meal times, stress responses, sleep patterns, and alcohol consumption.⁸ Combined with smartphone location data, the resulting dataset constitutes a detailed behavioral profile. The data originate from a medical device on the patient's body, travel through a consumer application, sit on commercial cloud servers, and reach third

parties with no connection to the patient's care.⁹ Figure 1 illustrates this data flow.

Three interrelated problems define this area. First, data-protection regulations contain gaps that leave substantial categories of diabetes device data without clear legal safeguards. Second, the question of who owns patient-generated health data (PGHD) remains unresolved, with patients, clinicians, device manufacturers, and software developers each asserting competing claims.¹⁰ Third, when researchers wish to repurpose these data, the consent frameworks in place often fail to explain what will happen to the data, who will access them, or for what purpose.¹¹ These three problems are usually treated

¹Instituto Nacional de Saúde Doutor Ricardo Jorge (INSA), Departamento de Promoção da Saúde e Prevenção de Doenças Não Transmissíveis, Lisboa, Portugal

Corresponding Author:

Paulo Dario, PhD, Instituto Nacional de Saúde Doutor Ricardo Jorge, Avenida Padre Cruz, Lisboa 1649-016, Portugal.
Email: paulo.dario@insa.min-saude.pt

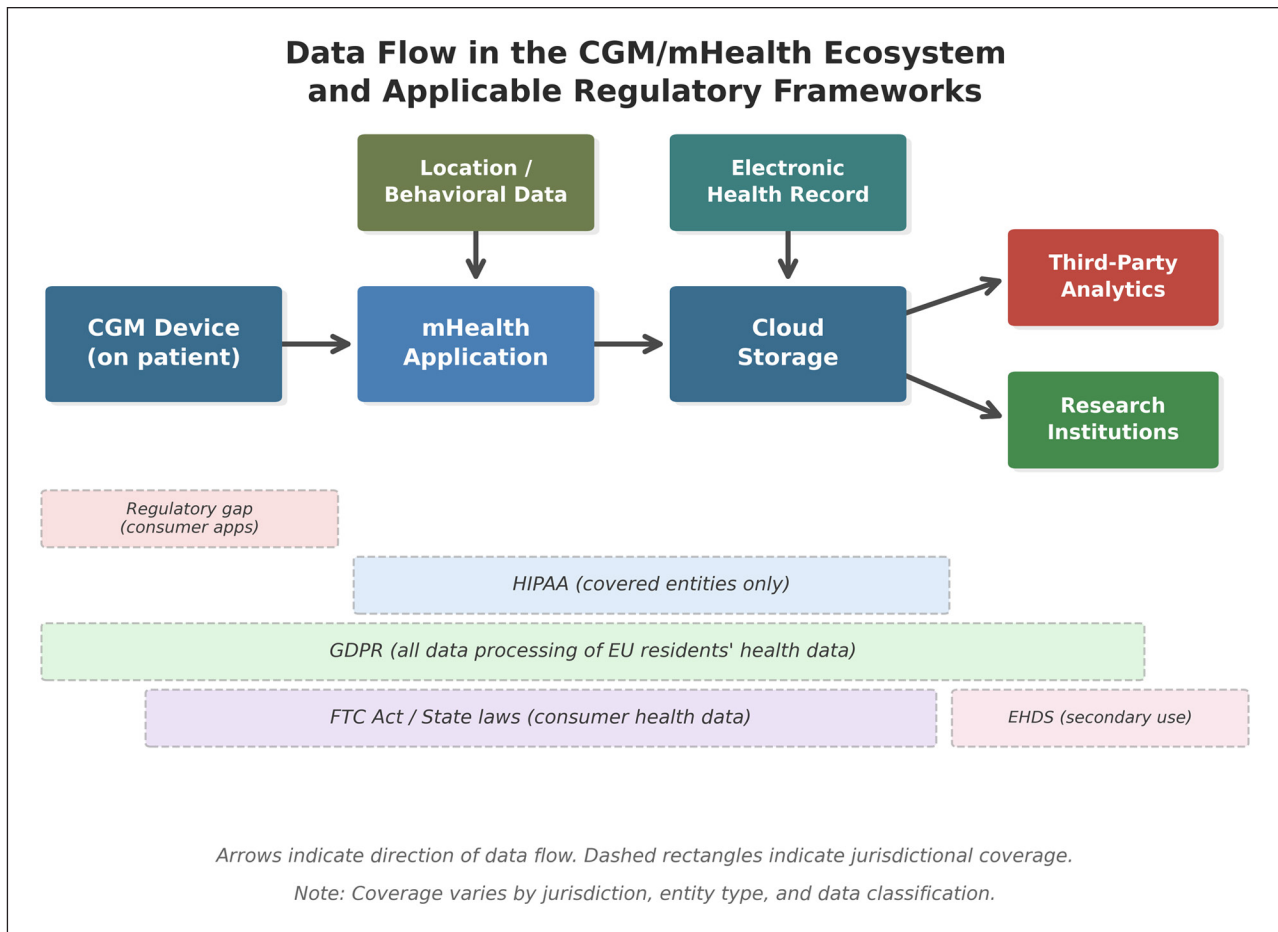


Figure 1. Data flow from CGM devices through mHealth applications to cloud storage, third-party analytics, and research institutions, with applicable regulatory frameworks. Dashed rectangles indicate jurisdictional coverage. Health Insurance Portability and Accountability Act's (HIPAA's) entity-based scope leaves a regulatory gap for consumer-grade applications. The GDPR covers all processing of European Union residents' health data regardless of entity type. The EHDS governs secondary use through Health Data Access Bodies (full implementation expected by 2029).

as separate domains; this review treats them together because each is logically dependent on the other two.

This review examines these three problems in the context of CGM and mHealth technologies for diabetes, surveys the regulatory frameworks in the United States (US) and the European Union (EU), and evaluates emerging technical and governance solutions that may help balance data-driven research against the protection of individual rights.

Data Privacy: Regulatory Frameworks and Their Limitations

The US Regulatory Environment

In the US, the Health Insurance Portability and Accountability Act (HIPAA) provides the primary legal framework for protecting health information. It applies to healthcare providers, health plans, healthcare clearinghouses, and their business associates.¹² The Privacy Rule governs how

protected health information may be used and disclosed, while the Security Rule establishes technical safeguards for electronic health data.

However, HIPAA's applicability to CGM and mHealth data is limited by its entity-based rather than data-based scope. Consumer health applications and wearable device manufacturers are generally not covered entities, meaning that glucose data transmitted from a CGM to a manufacturer's cloud platform, or shared with a third-party wellness application, may fall entirely outside HIPAA's protections.^{13,14} The Federal Trade Commission (FTC) has tried to fill some of this gap through enforcement actions under Section 5 of the FTC Act and an updated Health Breach Notification Rule (finalized in 2024) that explicitly includes health apps and connected devices.¹⁵ Some states have gone further. Washington's My Health My Data Act (2023), for instance, creates a private right of action that allows individuals to sue companies that collect or share their consumer health data without authorization.¹⁶ However, My Health My

Data Act (MHMDA) leaves the rules on permitted downstream uses of collected data incompletely defined; in practice, users are often required to grant broad data-use permissions to activate their CGM, which makes the consent obtained less meaningful than the statute implies. Connecticut, Nevada, and other states have introduced similar legislation, creating a trend toward state-level regulation that may produce a patchwork of obligations for CGM and mHealth companies.

Despite these developments, the US regulatory environment remains fragmented. A CGM user's glucose data may be governed by HIPAA when accessed by a clinician through an electronic health record, by the FTC Act when processed by the device manufacturer's application, and by state consumer protection laws when shared with third-party analytics services, or it may fall into a regulatory gap where none of these frameworks apply.^{9,13} A practical consequence is that CGM users cannot reliably anticipate which legal regime will govern any given use of their data, weakening informed consent.

The EU Regulatory Framework

The EU's General Data Protection Regulation (GDPR), in force since 2018, takes a fundamentally different approach by regulating data processing on the basis of the data itself rather than the entity processing it. Under GDPR, health data are classified as a special category of personal data subject to heightened protections, regardless of whether the data controller is a healthcare provider, a device manufacturer, or an application developer.¹⁷ Data subjects hold enforceable rights of access, rectification, erasure, and data portability. Processing of health data generally requires explicit consent or another specified legal basis.

The Medical Devices Regulation, applicable since May 2021, imposes additional requirements on devices that generate health data, including software for clinical decision support.¹⁸ Limited notified-body capacity has slowed enforcement, and transitional provisions extend MDR requirements to devices already on the market. Compliance costs also deter small and mid-sized firms from market entry. One recent analysis of 11 diabetes-management devices and apps marketed in Europe found that only 3 were registered in EUDAMED, and the privacy policies varied markedly in how transparent they were about data sharing.¹⁹ Of the 11 devices analyzed, a majority sent data to third parties for purposes unrelated to the user's care, and exercising GDPR rights often proved technically difficult.

Cross-Jurisdictional Challenges

The global nature of diabetes device networks creates additional complexities. A CGM manufactured in the US, used by a patient in the EU, and transmitting data to servers in a third jurisdiction is subject to multiple overlapping

regulatory regimes. Data transfer mechanisms such as Standard Contractual Clauses and adequacy decisions under GDPR impose constraints on cross-border data flows, but enforcement remains inconsistent.²⁰ Interoperability limitations compound this problem: A narrative commentary from EU, UK, and US perspectives documented how proprietary ecosystems and incompatible data formats impede cross-platform data sharing.²¹ For multinational clinical trials and registry studies aggregating CGM data across borders, these jurisdictional and technical barriers are practical obstacles to the secondary use of data for research.²² Table 1 compares these frameworks along scope, patient rights, coverage, and key limitations.

The cybersecurity of connected diabetes devices adds a further dimension. Insulin pumps and CGMs that communicate wirelessly are potentially vulnerable to data interception and, in a worst-case scenario, manipulation of dosing commands. The Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices (DTSec) and IEEE 2621 standards provide frameworks for wireless diabetes device security,²³ but adoption is uneven, and mandatory cybersecurity certification for diabetes devices transmitting health data remains absent in both the US and the EU.

Data Ownership: Competing Claims and Legal Ambiguity

The question of who owns health data generated by CGMs and mHealth applications has no clear legal answer in most jurisdictions. Unlike physical property, data do not fit neatly into existing ownership frameworks, and the concept of data ownership itself is contested among legal scholars.^{24,25} The need for clear medical data ownership laws has been articulated as a prerequisite for both translational research and patient empowerment.²⁶

In the US, healthcare providers own the physical medical record, while patients have a right of access to the information within it. HIPAA grants patients the right to request, view, and obtain copies of their health information, but this right of access does not equate to ownership.¹² For data generated by consumer CGMs and mHealth applications, control over data is typically governed by terms of service agreed to by the user at device activation or application download. Analyses of mHealth data-sharing practices have shown that health-related apps routinely transmit user data to third-party services, often for purposes unrelated to clinical care.²⁷ Studies of digital service agreements suggest that up to 97% of users accept such terms without reading them, transferring control of their data through a mechanism that does not reflect genuine informed decision-making.²⁸

The GDPR reframes the problem. Rather than establishing data ownership in a proprietary sense, the GDPR articulates a rights-based framework centered on the data subject. Individuals hold enforceable rights over the processing of their data, including the right to withdraw consent, the right

Table 1. Comparison of Regulatory Frameworks Governing CGM and mHealth Data.

Dimension	HIPAA (US)	FTC/State Laws (US)	GDPR (EU)	EHDS (EU)
Scope	Covered entities and business associates only	Consumer apps and devices not covered by HIPAA	All processing of EU residents' personal data	Secondary use of health data across EU member states
Data types	Protected health information (PHI)	Consumer health data (varies by state)	All health data (special category)	Electronic health data including device-generated data
Patient rights	Access and copy; no ownership right	Varies; WA MHMDA: consent required, private right of action	Access, rectification, erasure, portability, withdrawal of consent	Primary use: access, portability. Secondary: opt-out for certain uses
CGM/mHealth coverage	Limited: consumer devices typically excluded	Partial: FTC enforces for non-HIPAA health apps	Comprehensive: applies to all data controllers	Comprehensive: includes device data in EHR and registries
Enforcement	OCR; civil/criminal penalties	FTC enforcement; state attorneys general; private actions (WA)	National DPAs; fines up to 4% global turnover	Health Data Access Bodies; penalties per member state law
Key limitation	Entity-based: consumer devices fall outside scope	Fragmented patchwork; inconsistent across states	Enforcement inconsistency across member states; portability limited in practice	Full implementation not expected until 2029

Abbreviations: CGM, continuous glucose monitor; DPA, data-protection authority; EHDS, European Health Data Space; EHR, electronic health record; FTC, Federal Trade Commission; GDPR, General Data Protection Regulation; HIPAA, Health Insurance Portability and Accountability Act; mHealth, mobile health; OCR, Office for Civil Rights; WA MHMDA, Washington My Health My Data Act.

to erasure, and the right to data portability.¹⁷ The right to portability has been proposed as a mechanism to give patients with diabetes greater control over their CGM data by enabling them to transfer their data between devices and platforms.²⁹ In practice, however, interoperability barriers and proprietary data formats have limited the exercise of this right. Open-source initiatives such as Tidepool, which aims to standardize diabetes device data formats and enable cross-platform access,³⁰ aim to overcome these barriers, but adoption remains limited. Device manufacturers have little economic incentive to facilitate data portability, as data lock-in functions as a competitive advantage.^{19,31} User experience studies have confirmed that vendor lock-in remains a tangible barrier for patients attempting to access or transfer their own diabetes data.³²

The emergence of data cooperatives and patient-led data trusts offers an alternative governance model in which individuals collectively manage access to their health data.³³ Patients retain decision-making authority over data use, and any benefits from sharing are distributed according to collectively agreed terms. While nascent, these models address the power asymmetry between individual patients and device manufacturers.³⁴

There is also the question of derived data. Machine learning models trained on aggregated CGM readings generate predictions, risk scores, and treatment recommendations that are not the original data—they are something new. These derived insights can have commercial value independent of any one patient's contribution, yet regulatory frameworks do not address who owns or controls them.³⁵ The potential for

commercial exploitation is real, as mHealth data-sharing practices document routine transmission of user data to unrelated third parties.^{27,36} This is the central unresolved problem in current diabetes-data governance: Ownership rules designed for raw clinical records do not extend to the algorithmic products derived from them.

Secondary Use of Clinical Data for Research

The Promise

The secondary use of CGM and mHealth data for research could yield practical benefits. Large-scale CGM datasets have enabled validation of time in range as a meaningful clinical trial outcome measure and established associations between CGM-derived metrics and long-term complications such as diabetic retinopathy.^{37,38} Registry studies such as the Swedish National Diabetes Register and the T1D Exchange have demonstrated the value of aggregated clinical data in complementing randomized controlled trials.^{39,40} Data-driven approaches such as cluster analysis identifying distinct subgroups of adult-onset diabetes with differing complication profiles⁴¹ suggest that CGM-derived data could contribute to more individualized management.

Ethical Concerns

Secondary use of data raises 3 ethical concerns that are specific to the diabetes-technology context. The first relates to

consent. Most CGM users provide consent for data collection in the context of their clinical care or device use, but the scope of this consent with respect to future research applications is often ambiguous. Broad consent models, which authorize unspecified future uses of data, have been criticized for failing to meet the standard of informed consent, particularly when the future uses may include commercial research by the device manufacturer or its partners.^{42,43} Dynamic consent platforms, which allow individuals to make ongoing decisions about how their data are used, have been proposed as an alternative, though their practical implementation at scale remains limited.⁴⁴ Qualitative evidence suggests that adults with type 1 diabetes already exercise selective data sharing: Some choose not to use CGM remote-monitoring features due to concerns about anxiety, loss of independence, and insufficient customization of sharing options.⁴⁵

The second concern relates to deidentification. CGM data present particular challenges for anonymization due to their temporal density and potential linkage with behavioral and location data. A single CGM trace generates a temporally dense physiological signature that may suffice to reidentify an individual even after direct identifiers are removed. Time-series health data have been shown to be reidentifiable with high accuracy through pattern matching.^{46,47} A 2023 systematic review specifically examining deidentification of wearable device data concluded that current anonymization methods may give a false sense of security, as the temporal granularity of sensor-generated data creates unique individual signatures resistant to standard deidentification approaches.⁴⁸ The HIPAA Safe Harbor standard, which specifies 18 types of identifiers to be removed, was not designed with continuous physiological monitoring data in mind, and its adequacy for CGM datasets is questionable. A 2025 analysis of privacy policies across 17 leading wearable manufacturers found that 76% received high-risk ratings for transparency and that the majority shared data with third parties under terms that users were unlikely to understand.⁴⁹ The implication is that ‘deidentified’ CGM datasets should be treated as identifiable for governance purposes; the question is no longer whether reidentification is possible, but how to manage the risk.

The third concern involves the boundary between research and commercial exploitation. Device manufacturers that collect CGM data for product improvement may also use those data, or insights derived from them, for commercial applications such as development of proprietary algorithms or sale of aggregated analytics to pharmaceutical companies and insurers.^{27,36} When research and commercial objectives converge within the same data environment, the distinction between use that benefits the patient community and use that primarily serves corporate interests becomes difficult to maintain.

The European Health Data Space

The European Health Data Space (EHDS) regulation, published in the Official Journal of the EU on March 5, 2025, is

the most detailed legislative effort to date to create a governance framework for secondary use of health data.⁵⁰ The EHDS establishes Health Data Access Bodies in each member state to evaluate and authorize requests for secondary use of health data, including scientific research and public health surveillance. Data access must occur through secure processing environments, and certain uses, including insurance risk assessment and direct marketing, are prohibited.⁵¹

For diabetes research, the EHDS could facilitate cross-border studies using CGM and mHealth data while maintaining consistent governance standards across member states. However, implementation challenges remain substantial, including the need to harmonize data formats across different CGM platforms, establish interoperability standards for mHealth applications, and build the institutional infrastructure required to operate Health Data Access Bodies effectively in each member state. Efforts such as the iCoDE-2 standards project, which aims to integrate connected diabetes device data into electronic health records through standardized formats, illustrate both the potential and the complexity of achieving interoperability in this domain.⁵² The timeline for implementation is phased: While the regulation entered into force on March 26, 2025, the full application of secondary use provisions is not expected until 2029, leaving a multi-year gap during which current fragmented approaches will continue to govern research access to diabetes device data.^{50,53}

Emerging Technical Solutions

Technical approaches to privacy preservation offer a complementary path to regulatory reform. Federated learning, in which machine learning models are trained on decentralized data without the data leaving the local institution, has been applied to diabetes prediction and classification tasks with results comparable to centralized approaches.^{54,55} Differential privacy, which introduces calibrated noise into datasets or model outputs to prevent the identification of individual records, has been combined with federated learning in diabetes-specific implementations.⁵⁶ Homomorphic encryption, which allows computation on encrypted data, and synthetic data generation, which creates artificial datasets preserving the statistical properties of the original, are additional privacy-enhancing technologies (PETs) that may enable research on sensitive CGM data without exposing individual records.⁵⁷

These technical solutions have important limitations. Federated learning introduces communication overhead and may produce models biased toward institutions with larger datasets. Differential privacy involves an inherent trade-off between privacy protection and data utility, and the appropriate calibration of noise parameters for glucose data has not been established. Synthetic data may fail to capture rare but clinically relevant patterns, such as nocturnal hypoglycemia episodes. No technical solution eliminates the need for appropriate governance and consent frameworks; PETs should be

Table 2. Recommended Actions to Address Privacy, Ownership, and Secondary-Use Gaps in CGM and mHealth data.

#	Stakeholder	Recommended action	Specific implementation step
1	US Congress and EU institutions	Extend health-data protections to all entities processing medical-device data, irrespective of covered-entity status	Amend HIPAA (or enact a federal equivalent) to define protected health information by data type rather than by entity; align GDPR enforcement to consumer-grade CGM and mHealth platforms
2	Device manufacturers and software developers	Adopt interoperability and data-portability standards as a release-blocking requirement	Conform to iCoDE-2 specifications for EHR integration and to Tidepool open-source data formats; provide standardized export and portability APIs at product approval
3	Researchers, IRBs, and EHDS Health Data Access Bodies	Make privacy-enhancing technologies the default for secondary analysis of CGM data	Require federated learning, differential privacy, or equivalent PETs in the standard IRB or HDAB review checklist; reject protocols that centralize raw CGM records without explicit justification
4	Funders, sponsors, and IRBs	Replace static broad consent with dynamic consent for connected diabetes-technology studies	Mandate dynamic consent platforms in protocols using CGM or mHealth data, allowing participants to grant, modify, or withdraw permission per use category over time
5	Regulators and AID-system manufacturers	Develop privacy and cybersecurity rules specific to closed-loop automated insulin-delivery systems	Issue AID-specific guidance covering real-time CGM, controller, and pump data flows; require certification under DTSec or IEEE 2621 (or equivalent) before market authorization

Abbreviations: AID, automated insulin delivery; API, application programming interface; CGM, continuous glucose monitor; DTSec, Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices; EHDS, European Health Data Space; EHR, electronic health record; GDPR, General Data Protection Regulation; HDAB, Health Data Access Body; HIPAA, Health Insurance Portability and Accountability Act; IEEE 2621, IEEE Standard for Wireless Diabetes Device Security; IRB, institutional review board; mHealth, mobile health; PET, privacy-enhancing technology.

understood as tools that expand the range of options available within a broader governance structure.^{58,59}

Blockchain-based approaches to consent management and data provenance tracking have also attracted interest in this area. By recording data access events on a distributed ledger, blockchain systems could provide patients with an auditable record of who has accessed their CGM data, when, and for what stated purpose. Proof-of-concept implementations have been described, though scalability concerns, energy consumption, and the tension between immutable records and the GDPR right to erasure remain barriers that require careful architectural design.^{35,57}

Conclusions

The rapid adoption of CGMs and mHealth applications in diabetes management has created a data environment that outpaces the regulatory, legal, and ethical frameworks designed to govern it. The data produced by these devices are simultaneously clinical records, consumer data, and commercial assets, and the boundaries between these categories are poorly defined by existing law. Privacy protections remain fragmented, with significant gaps for consumer-grade devices that fall outside HIPAA and face inconsistent enforcement under GDPR. Data ownership remains legally ambiguous, and current consent mechanisms fail to provide patients with meaningful control over how their data are used. This review focuses on the US and EU regulatory

environments; other major diabetes populations, including those in China, India, and Brazil, face distinct regulatory challenges that warrant separate analysis.

Secondary use of diabetes device data for research can improve clinical outcomes, but not responsibly without addressing ethical concerns around consent, de-identification, and the conflation of research with commercial interests. The EHDS is the largest effort to date to create a coherent governance framework for secondary use of health data, though its effectiveness will depend on how well member states implement it and whether they invest in the required institutional infrastructure.

Five actions follow from this analysis and are summarized in Table 2.

The people who wear these devices and generate these data need a framework that protects their privacy and autonomy without blocking the research that may improve their care. Without one, the default is an unregulated environment in which commercial interests set the terms of access and use, and in which the trust that sustains both clinical adoption and research participation steadily erodes.

Abbreviations

AID, automated insulin delivery; CGM, continuous glucose monitor; EHDS, European Health Data Space; EHR, electronic health record; EU, European Union; FDA, Food and Drug Administration; FTC, Federal Trade Commission; GDPR, General Data Protection Regulation; HIPAA, Health Insurance Portability and Accountability

Act; MDR, Medical Devices Regulation; mHealth, mobile health; OTC, over-the-counter; PET, privacy-enhancing technology; PGHD, patient-generated health data; US, United States

Acknowledgments

As a non-native English speaker, the author used Anthropic Claude (AI assistant) for language editing and reference verification during manuscript preparation. The author retains full responsibility for all content.

ORCID iD

Paulo Dario  <https://orcid.org/0000-0002-4203-9179>

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

1. Battelino T, Danne T, Bergenstal RM, et al. Clinical targets for continuous glucose monitoring data interpretation: recommendations from the International Consensus on Time in Range. *Diabetes Care*. 2019;42(8):1593-1603.
2. Klonoff DC. The current status of mHealth for diabetes: will it be the next big thing? *J Diabetes Sci Technol*. 2013;7(3):749-758.
3. Fleming GA, Petrie JR, Bergenstal RM, Holl RW, Peters AL, Heinemann L. Diabetes digital app technology: benefits, challenges, and recommendations. A consensus report by the European Association for the Study of Diabetes and the American Diabetes Association Diabetes Technology Working Group. *Diabetes Care*. 2020;43(1):250-260.
4. American Diabetes Association Professional Practice Committee. Standards of care in diabetes - 2024. *Diabetes Care*. 2024;47(suppl 1):S1-S321.
5. Danne T, Nimri R, Battelino T, et al. International consensus on use of continuous glucose monitoring. *Diabetes Care*. 2017;40(12):1631-1640.
6. U.S. Food and Drug Administration. FDA clears first over-the-counter continuous glucose monitor. FDA News Release. March 5, 2024. Accessed March 2026. <https://www.fda.gov/news-events/press-announcements/fda-clears-first-over-counter-continuous-glucose-monitor>
7. Grand View Research. *Continuous glucose monitoring devices market size, share & trends analysis report, 2025-2033*. Grand View Research; 2024.
8. Britton KE, Britton-Colonnese JD. Privacy and security issues surrounding the protection of data generated by continuous glucose monitors. *J Diabetes Sci Technol*. 2017;11(2):216-219.
9. Theodos K, Sittig S. Health information privacy laws in the digital age: HIPAA doesn't apply. *Perspect Health Inf Manag*. 2021;18(Winter):11.
10. Conduah AK, Ofuo S, Siaw-Marfo D. Data privacy in healthcare: global challenges and solutions. *Digit Health*. 2025;11:20552076251343959.
11. Galvin HK, DeMuro PR. Developments in privacy and data ownership in mobile health technologies, 2016-2019. *Yearb Med Inform*. 2020;29(1):32-43. doi:10.1055/s-0040-1701987
12. U.S. Department of Health and Human Services. Summary of the HIPAA privacy rule. Accessed March 2026. <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
13. Martinez-Martin N, Kreitmair K. Ethical issues for direct-to-consumer digital psychotherapy apps: addressing accountability, data protection, and consent. *JMIR Ment Health*. 2018;5(2):e32.
14. Nebeker C, Torous J, Bartlett Ellis RJ. Building the case for actionable ethics in digital health research supported by artificial intelligence. *BMC Med*. 2019;17(1):137.
15. Federal Trade Commission. Health Breach Notification Rule: final rule. *Fed Regist*. 2024;89(82):32794-32834.
16. Washington State Legislature. My Health My Data Act, HB 1155, 2023.
17. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Off J Eur Union*. 2016;L119:1-88.
18. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices (Medical Devices Regulation). *Off J Eur Union*. 2017;L117:1-175.
19. Randine P, Pocs M, Cooper JG, et al. Privacy concerns related to data sharing for European diabetes devices. *J Diabetes Sci Technol*. 2025;19(3):611-619.
20. Bradford L, Aboy M, Liddell K. International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an adequate level of protection. *J Law Biosci*. 2020;7(1):lsaa055.
21. Jendle J, Adolfsson P, Choudhary P, et al. A narrative commentary about interoperability in medical devices and data used in diabetes therapy from an academic EU/UK/US perspective. *Diabetologia*. 2024;67(2):236-245. doi:10.1007/s00125-023-06049-5
22. Dove ES, Knoppers BM, Zawati MH. Towards an ethics safe harbor for global biomedical research. *J Law Biosci*. 2014;1(1):3-51.
23. Klonoff DC, Kleidermacher DN. Now is the time for a cybersecurity standard for connected diabetes devices. *J Diabetes Sci Technol*. 2016;10(3):623-626.
24. Rodwin MA. The case for public ownership of patient data. *JAMA*. 2009;302(1):86-88.
25. Blasimme A, Vayena E. The ethics of AI in biomedical research, patient care, and public health. In: Dubber MD, Pasquale F, Das S, eds. *The Oxford Handbook of Ethics of AI*. Oxford University Press; 2020:703-718. doi:10.1093/oxfordhdb/9780190067397.013.45
26. Klonoff DC, Scheideman AF, Shao MM, et al. The need for clear medical data ownership laws. *J Transl Med*. 2026;24(1):5. doi:10.1186/s12967-025-07486-z
27. Grundy Q, Chiu K, Held F, Continella A, Bero L, Holz R. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *BMJ*. 2019;364:1920.

28. Obar JA, Oeldorf-Hirsch A. The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. *Inf Commun Soc*. 2020;23(1):128-147.
29. De Hert P, Papakonstantinou V, Malgieri G, Beslay L, Sanchez I. The right to data portability in the GDPR: towards user-centric interoperability of digital services. *Comput Law Secur Rev*. 2018;34(2):193-203.
30. Neinstein A, Wong J, Look H, et al. A case study in open source innovation: developing the Tidepool Platform for interoperability in type 1 diabetes management. *J Am Med Inform Assoc*. 2016;23(2):324-332. doi:10.1093/jamia/ocv104
31. Randine P, Kopperstad Wolff M, Pocs M, et al. Unlocking real-time data access in diabetes management: toward an interoperability model. *J Diabetes Sci Technol*. Published online March 28, 2025. doi:10.1177/19322968251327602
32. Randine P, Arsand E. User experience and vendor lock-in with current diabetes information system. *Stud Health Technol Inform*. 2025;327:682-686.
33. Delacroix S, Lawrence ND. Bottom-up data trusts: disturbing the 'one size fits all' approach to data governance. *Int Data Priv Law*. 2019;9(4):236-252.
34. Kish LJ, Topol EJ. Unpatients - why patients should own their medical data. *Nat Biotechnol*. 2015;33(9):921-924.
35. Price WN 2nd, Cohen IG. Privacy in the age of medical big data. *Nat Med*. 2019;25(1):37-43.
36. Grundy Q. A review of the quality and impact of mobile health apps. *Annu Rev Public Health*. 2022;43:117-134.
37. Beck RW, Bergenstal RM, Riddlesworth TD, et al. Validation of time in range as an outcome measure for diabetes clinical trials. *Diabetes Care*. 2019;42(3):400-405.
38. Lu J, Ma X, Zhou J, et al. Association of time in range, as assessed by continuous glucose monitoring, with diabetic retinopathy in type 2 diabetes. *Diabetes Care*. 2018;41(11):2370-2376.
39. Lind M, Svensson AM, Kosiborod M, et al. Glycemic control and excess mortality in type 1 diabetes. *N Engl J Med*. 2014;371(21):1972-1982.
40. Beck RW, Tamborlane WV, Bergenstal RM, Miller KM, DuBose SN, Hall CA. The T1D Exchange clinic registry. *J Clin Endocrinol Metab*. 2012;97(12):4383-4389. doi:10.1210/jc.2012-1561
41. Ahlqvist E, Storm P, Käräjämäki A, et al. Novel subgroups of adult-onset diabetes and their association with outcomes: a data-driven cluster analysis of six variables. *Lancet Diabetes Endocrinol*. 2018;6(5):361-369.
42. Sheehan M. Can broad consent be informed consent? *Public Health Ethics*. 2011;4(3):226-235.
43. Ploug T, Holm S. Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research. *BMJ*. 2015;350:h2146.
44. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: a patient interface for twenty-first century research networks. *Eur J Hum Genet*. 2015;23(2):141-146.
45. Rathan A, Boucsein A, Crockett H, Wheeler BJ. Continuous glucose monitoring remote monitoring does not meet the needs of all adult users: a qualitative study. *Diabet Med*. 2025;42(10):e70120.
46. Na L, Yang C, Lo CC, Zhao F, Fukuoka Y, Aswani A. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. *JAMA Netw Open*. 2018;1(8):e186040.
47. Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun*. 2019;10(1):3069.
48. Chikwetu L, Miao Y, Woldetensae MK, Bell D, Goldenholz DM, Dunn J. Does deidentification of data from wearable devices give us a false sense of security? A systematic review. *Lancet Digit Health*. 2023;5(4):e239-e247. doi:10.1016/S2589-7500(22)00234-5
49. Doherty C, Baldwin M, Lambe R, Altini M, Caulfield B. Privacy in consumer wearable technologies: a living systematic analysis of data policies across leading manufacturers. *NPJ Digit Med*. 2025;8(1):363. doi:10.1038/s41746-025-01757-1
50. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. Official Journal of the European Union, March 5, 2025. Accessed May 19, 2026. <http://data.europa.eu/eli/reg/2025/327/oj>
51. European Commission. European Health Data Space Regulation (EHDS). Accessed March 2026. https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en
52. Aaron RE, Tian T, Yeung AM, Huang J, Klonoff DC, Espinoza JC. The launch of the iCoDE-2 standard project: integration of connected diabetes device data into the electronic health record. *J Diabetes Sci Technol*. 2024;18(1):82-88.
53. Council of the European Union. European Health Data Space: council adopts new rules on the use of health data. Press release 16453/24. December 2024. Accessed March 2026. <https://www.consilium.europa.eu/en/press/press-releases/2024/12>
54. Jayalakshmi R, Tamilvizhi T. Privacy preservation in diabetic disease prediction using federated learning based on efficient cross stage recurrent model. *Sci Rep*. 2025;15:37258. doi:10.1038/s41598-025-21229-6
55. Moshawrab M, Adda M, Bouzouane A, Ibrahim H, Raad A. Reviewing federated machine learning and its use in diseases prediction. *Sensors*. 2023;23(4):2112. doi:10.3390/s23042112
56. Moulahi W, Jdey I, Moulahi T, Alawida M, Alabdulatif A. A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. *Comput Biol Med*. 2023;167:107630. doi:10.1016/j.compbiomed.2023.107630
57. Kaissis GA, Makowski MR, Ruckert D, Braren RF. Secure, privacy-preserving and federated machine learning in medical imaging. *Nat Mach Intell*. 2020;2(6):305-311.
58. Li T, Sahu AK, Talwalkar A, Smith V. Federated learning: challenges, methods, and future directions. *IEEE Signal Process Mag*. 2020;37(3):50-60.
59. Vayena E, Blasimme A, Cohen IG. Machine learning in medicine: addressing ethical challenges. *PLoS Med*. 2018;15(11):e1002689.