RISING T1DE ALLIANCE

CGM Data Policy Initiative

A Cross-Sector Framework for CGM Data Access, Interoperability, and Governance

October 2026

Prepared by:
Dominique Pahud, MBA & Juan Espinoza, MD
on behalf of the Rising T1DE Alliance CGM Data Policy Initiative Working Group

Authorship, Funding, & Publication Information

CGM Data Policy Initiative: A Cross-Sector Framework for CGM Data Access, Interoperability, and Governance.
Published online by the Rising T1DE Alliance on October 5, 2026.
Version 1.0

Lead Authors

- Dominique Pahud, MBA | Oros AI LLC
- Juan Espinoza, MD | Ann & Robert H. Lurie Children's Hospital of Chicago

Group Authorship
This report was prepared on behalf of the Rising T1DE Alliance CGM Data Policy Initiative Working Group. The Working Group served as the collective authorship group for this initiative, informing the development, refinement, and review of the policy framework and recommendations through the process described in this report.

Lead Author Disclosures

- DP reports consulting fees from Children's Mercy Kansas City and Ann & Robert H. Lurie Children's Hospital of Chicago, funded through a Helmsley Charitable Trust grant to Lurie Children's Hospital in support of the Rising T1DE Alliance.
- JE receives grant funding from NIH and FDA, and serves as Principal Investigator on a grant from the Helmsley Charitable Trust to Ann & Robert H. Lurie Children's Hospital of Chicago. He has received consulting fees from Dexcom, Glooko, and Sanofi.

Suggested Citation (AMA format)
Pahud D, Espinoza J, Rising T1DE Alliance CGM Data Policy Initiative Working Group. C*GM Data Policy Initiative: A Cross-Sector Framework for CGM Data Access, Interoperability, and Governance*. Version 1.0. Rising T1DE Alliance; 2026. www.risingt1dealliance.org/cgm-data-policy.

Funding
This work was made possible with funding and support from The Leona M. and Harry B. Helmsley Charitable Trust.



Contributors

The individuals named below participated in one or more Working Group Meetings and supporting engagements, including the development of the CGM Data Dictionary (Appendix A). Participants are listed by default, with organizational affiliation at the time of participation; participants had the option to choose not to be named. Participation does not imply endorsement of the recommendations.

Rising T1DE Alliance Project Team

- Dominique Pahud, Juan Espinoza, Angel Avina, Andrew Berry, Jordan Cashwell, Grace Garcia, Sadaf Javaid, Kendall Job, Lawrence Lett, Brent Lockee, Dan Tilden, Eric Williams, Jr.

Industry

- Abbott: Jeff Draper, Alexa Engle, Jacob Sunol, Naunihal Virdi
- Dexcom: Alexandra Bortnick, Molly Malloy, Beata Piehl
- DreaMed: Paul Schroeder
- Glooko: Mark Clements, Rich Glenn, Dan Korelitz, Markus Svensson
- Medtronic: Scott Hebl, Diana Miller, Robert Vigersky
- Senseonics: Francine Kaufman, Hari Sree
- Tidepool: Brandon Arbiter, Rea Rostosky, Kelly Watson, Eric Wollesen, Bill Zeller

Patient Advocacy, Patients, and Caregivers

- American Diabetes Association: Jess Pius-Nwagwu
- Breakthrough T1D, formerly JDRF: Aaron Turner-Phifer
- Diabetes Leadership Council: Erin Callahan
- The diaTribe Foundation: Mareda Lewer
- National Health Council: Omar Escontrias, Silke Schoch
- T1D Exchange: Suzanne McKee, Dave Walton
- Patient and caregiver participants: Christine Fallabel (person living with type 1 diabetes), Julie Hoffman (caregiver and advocate), Alyssa Phillips (person living with type 1 diabetes)

National Committee for Quality Assurance (NCQA)

- Caroline Blaum, Kaila Boyd, Nikko Gutierrez, Emily Hubbard, Brenna Lin, Mia Nievera

The Helmsley Charitable Trust

- Laurel Koester, Sean Sullivan, Serena Thadani

We are especially grateful to the people living with diabetes and caregivers who participated in the panel surveys that informed this work.

Endorsements

The following organizations endorse the recommendations in this paper. Endorsement indicates support for the six recommendations; it does not imply agreement with every element of the paper, nor participation in the Working Group.

- Breakthrough T1D, formerly JDRF
- Diabetes Leadership Council
- Diabetes Patient Advocacy Coalition
- Diabetes Technology Society
- The diaTribe Foundation
- International Diabetes Center HealthPartners Institute
- National Health Council
- T1D Exchange

How to Read This Document

Section 1 introduces the clinical and policy problem. Section 2 reviews the federal and state policy landscape relevant to CGM data. Section 3 describes our mixed-methods engagement process. Section 4 presents the relevant perspectives of patients and caregivers across three surveys. Section 5 summarizes findings from the cross-sector Working Group Meetings. Section 6 presents the six policy recommendations, each with rationale, participant input, tradeoffs and alternatives considered, a proposed implementation pathway, and an at-a-glance summary. Section 7 concludes by drawing out how the recommendations reinforce one another and closes with proposed next steps to advance the work. Appendices contain the working CGM data dictionary, shared contracting principles, alignment with the CMS Interoperability Framework, the public comments we submitted to federal agencies, and a glossary of terms and abbreviations.

Table of Contents

Authorship, Funding, & Publication Information 2
Contributors 3
Endorsements 4
How to Read This Document 5
Table of Contents 6
Executive Summary 9
Policy Recommendations 9
Patient Voice 10
Next Steps 11
Plain Language Summary 12
1. Introduction 14
2. Policy Landscape 16
2.1 The Federal Foundation 16
2.2 The Recent Regulatory Wave 17
2.3 The CMS Interoperability Framework 19
2.4 Reimbursement and Care-Delivery Context 19
2.5 State-Level Activity 21
2.6 Voluntary and Non-governmental Frameworks 21
2.7 The Gap That Remains 23
3. Methods and Engagement Process 24
3.1 Regulatory Landscape Review 24
3.2 Federal Regulatory Policy Engagement 24
3.3 Cross-Sector Working Group Meetings 24
3.4 Patient and Advocate Engagement 26
3.5 Implementation Workstreams 26
3.6 Analysis and Synthesis 26
3.7 Limitations and Exclusions 27
4. Patient and Caregiver Perspectives 28
4.1 Survey Methods 28
4.2 Who Responded 29
4.3 Survey 1: Access, Coordination, and the Limits of Data Use 31
4.4 Survey 2: Data Use, Trust, and What Patients Want From Their Care Team 32
4.5 Survey 3: From What to How 35

4.6 Voices from the Community....37
4.7 What We Heard Across All Three Surveys....37
5. Working Group Findings....39
5.1 Areas of Alignment....39
5.2 Areas of Alignment with Open Questions....40
5.3 Participant Perspectives....41
5.4 What the Working Group Confirmed....42
6. Policy Recommendations....43
6.1 Implementation Pathways....43
6.2 Recommendation Summary....44
6.3 Recommendation 1: Clarify patient access rights for device data....45
6.4 Recommendation 2: Extend interoperability standards to CGM data....48
6.5 Recommendation 3: Extend information-blocking protections to device platforms....51
6.6 Recommendation 4: Define baseline infrastructure expectations....55
6.7 Recommendation 5: Develop shared contracting principles....59
6.8 Recommendation 6: Develop and maintain a shared CGM data dictionary....62
7. Conclusions and Next Steps....66
A Foundation for Future Work....66
Next Steps....67
Closing....68
References....69
Appendix A: CGM Data Dictionary....72
Summary Alignment Table....73
Cross-Cutting Findings....74
Status and Confirmation....75
Appendix B: Shared Contracting Principles....76
B.1 EHR Integration Permissions....76
B.2 Multi-Device Data Chain (Consent Portability)....76
B.3 Data Granularity....76
B.4 Downstream Sharing Restrictions....77
B.5 Summary....77
Appendix C: CMS Interoperability Framework Alignment....78
C.1 CMS Framework Domains....78
C.2 Recommendation-to-Criteria Mapping....78
C.3 Detailed Alignment Rationale....79

Appendix D: CMS RFI Response 81
Executive Summary 81
Recommendations by RFI Section 81
Supporting Policy Framework 82
Phased Implementation 82
Appendix E: HTI-5 Public Comments 83
Executive Summary 83
Four Specific Recommendations 83
Why This Matters for Diabetes Device Data Integration 84
Appendix F: Glossary of Terms and Abbreviations 85

Executive Summary

Abbreviations used throughout this paper, including iCoDE, EHR, FHIR, USCDI and LOINC, are defined in Appendix F: Glossary of Terms and Abbreviations.

Continuous glucose monitoring (CGM) has transformed diabetes care. Real-time glucose data enable more precise insulin dosing, reduce hypoglycemia, and improve outcomes for people living with type 1 and type 2 diabetes. The infrastructure for using these data has also advanced, reflecting broader progress in health data interoperability and important milestones such as the iCoDE standards in 2022. Major CGM manufacturers and data aggregators have increasingly brought EHR integrations to market. Yet CGM has become part of routine diabetes care faster than the data infrastructure around it has evolved, leaving CGM data largely distributed across proprietary device ecosystems rather than routinely integrated into the EHR. Patients struggle to share their device data across care settings or exercise meaningful control over how it is used. Clinicians work without the full picture. Most health systems cannot yet build the population-level workflows that CGM data makes possible; the few that have, have done so through bespoke integration rather than shared infrastructure.

The building blocks of a federal regulatory framework for health data access and interoperability are already in place. HIPAA and HITECH established patient access rights, the 21st Century Cures Act prohibited information blocking by defined actors, and ONC established certification criteria and interoperability standards for health IT. Among technology developers, however, the information-blocking framework generally reaches developers of certified health IT, leaving many CGM manufacturers and device-data platforms outside that actor category**.** Recent federal policy signals suggest that this gap may be beginning to narrow. The HTI-5 proposed rule reinforces an API-first direction for certified systems, early indications around HTI-6 point toward greater attention to device data, and the CMS Interoperability Framework, released in July 2025, offers a voluntary blueprint that touches nearly every domain relevant to CGM data exchange. Together, these developments create a timely policy opportunity to extend interoperability principles more fully to CGM data.

This white paper presents consensus-driven recommendations from a cross-sector process convened by the Rising T1DE Alliance (RTA). Through a series of Working Group Meetings beginning in June 2025, we brought together CGM device manufacturers, data aggregators, patient advocacy organizations, patients and caregivers, the National Committee for Quality Assurance, and the Helmsley Charitable Trust. This process was informed by three patient surveys that captured the priorities of people living with diabetes and caregivers, and it was further shaped through engagement with emerging federal policy, including a formal response to the May 2025 CMS-ONC Request for Information and public comments on the HTI-5 Proposed Rule. Together, these activities provided the foundation for the recommendations presented here.

Policy Recommendations

We propose six policy recommendations grounded in existing laws and regulatory authorities. Together they advance a single principle, that medical device data should align with the regulatory frameworks

governing electronic health information and interoperable health IT, particularly in patient access, data sharing, interoperability, and information-blocking protections.

1. **Clarify patient access rights for device data:** Clarify how existing HIPAA and HITECH access rights apply to CGM and other device data, so individuals can direct their device data to any provider or third party they choose.
2. **Extend interoperability standards to CGM data:** Adopt modern API standards (FHIR preferred, HL7v2 messaging acceptable) and expand USCDI to include the essential CGM data elements needed for safe, meaningful exchange.
3. **Extend information-blocking protections to device platforms:** Clarify whether and how these protections reach device manufacturers and intermediaries, with safeguards that balance patient access against safety and intellectual-property concerns.
4. **Define baseline infrastructure expectations:** Set expectations for device-data platforms that promote consistency, safety, interoperability, and patient-centered access.
5. **Develop shared contracting principles:** Align on principles that reduce the time and cost of putting data-sharing agreements in place across manufacturers, aggregators, and health systems, while respecting intellectual property and patient rights.
6. **Develop and maintain a shared CGM data dictionary:** Establish consistent definitions, calculation methods, and terminology, aligned with USCDI, LOINC, iCoDE, and the AGP specification.

Each recommendation's rationale, participant input, tradeoffs and alternatives considered, proposed implementation pathway, and an at-a-glance summary appear in Section 6.

Patient Voice

Three survey waves reaching a highly engaged panel of people living with type 1 diabetes and caregivers highlighted several cross-cutting themes:

- **"Use my data to help me, not control me."** Strong willingness to share CGM data for research and care improvement coexists with firm opposition to punitive insurer uses. Only 11 percent accept use for eligibility or prior authorization; only 9 percent accept use for premiums or cost-sharing.
- **Trust requires transparency, consent, and safeguards.** Opt-out rights (74 percent), transparency about use (76 percent), de-identification (65 percent), explicit consent (61 percent), and return of findings (63 percent) are the guardrails patients want. Only 9 percent are comfortable with no additional safeguards.
- **Patients want action and support, not just access.** Only one in three feels well-informed about their CGM data. Fifty-two percent want help using the data for better daily decisions; 70 percent want personalized recommendations based on CGM trends; 52 percent want proactive outreach when concerning patterns emerge.

Next Steps

CGM data is becoming foundational infrastructure for proactive, coordinated, patient-centered chronic care, and this paper offers a framework intended as a starting point for deeper work. Multiple federal agencies are actively examining health data integration, including through the anticipated HTI-6 rulemaking, which creates an opportunity to align device-data expectations with the protections that already govern other electronic health information. Substantial work remains to refine and operationalize these recommendations. We offer them to policymakers, regulators, manufacturers and data aggregators, health systems, quality organizations, payers, and patient advocacy partners as a basis for continued collaboration.

Plain Language Summary

Continuous glucose monitors (CGMs) are wearable sensors that measure glucose levels throughout the day and night. CGMs have changed diabetes care, but the data systems around it have not kept up. Most people can see their glucose data in a device app or web portal. But those data do not always move easily into the electronic health record or from one care setting to another. This can leave care teams with an incomplete view. It can also make it harder to reach patients between visits and can force patients to manage data sharing on their own.

The main gap is not a lack of health data rules. Federal law already gives patients many rights to access health information, and federal rules support electronic data sharing. But those protections depend on who holds the data. They often apply once CGM data are in a health system. Device makers and device data platforms may sit outside the same rules. At the same time, the basic tools needed to move CGM data already exist. The challenge is to make access and sharing more consistent, practical, and centered on patient needs.

What we did

The Rising T1DE Alliance brought together CGM companies, data companies, patient groups, people living with diabetes and caregivers, quality experts, and other partners. From 2025 through 2026, we held five working group meetings across these groups, ran three patient and caregiver surveys, reviewed federal policy, and submitted comments to federal agencies. We also created two practical tools: a shared CGM data dictionary and shared principles for data-sharing agreements.

What we recommend

The report proposes six connected actions:

1. **Clarify patient access rights.** Clarify how existing rights apply to CGM and other device data, including a patient's ability to send data to providers and trusted third parties.
2. **Use common technical standards.** Make it easier for CGM data to move between systems, with FHIR as the preferred approach, and add key CGM data elements to national health data standards.
3. **Strengthen protections against barriers to data sharing.** Apply stronger protections against practices that unfairly limit access to or sharing of device data, while protecting safety, privacy, and intellectual property.
4. **Set basic expectations for device-data platforms.** Define capabilities such as secure access, audit logs, reliable data connections, and patient-directed sharing.
5. **Reduce contracting barriers.** Use shared principles so CGM companies, data companies, and health systems do not have to renegotiate the same basic issues for each new connection.
6. **Use consistent definitions.** Maintain a shared CGM data dictionary so important measures are defined and calculated in ways that can be compared across systems.

These recommendations use existing federal authority, standards, guidance, and voluntary industry action rather than new legislation. They also reflect what survey participants told us. Participants want CGM data to support better care and research. They also want clear information about how their data are used, real choices about sharing, and safeguards against uses that could harm access to coverage.

What comes next

The next step is to put these ideas into practice. Federal agencies can clarify access rules and advance common standards. CGM companies and data platforms can adopt common technical approaches, data definitions, and contracting principles. Health systems can use those tools to bring CGM data into routine care and population health programs. Patients and caregivers should remain part of these decisions.

Some issues still need more work. These include how consent and data-use choices should follow a patient across systems, which platform capabilities should be a common minimum, and how standard CGM measures could support future quality measurement. The larger goal is simple: CGM data should be available, understandable, and useful wherever a person receives care.

1. Introduction

Continuous glucose monitoring (CGM) has transformed diabetes care over the last two decades. CGM devices provide real-time glucose readings and trend data that enable more precise insulin dosing, reduce hypoglycemia, and improve glycemic outcomes for people with type 1 and type 2 diabetes.[1] Adoption has accelerated markedly: Medicare coverage expansion in 2017 and subsequent commercial payer uptake have extended access to increasingly diverse populations.[2] The clinical and quality-of-life benefits of real-time monitoring and trend data have made CGM an essential tool in modern diabetes management and part of the standard of care.

Despite these clinical advances, CGM data often remain siloed in proprietary systems, disconnected from the electronic health record where clinicians document care and make treatment decisions.[3] This fragmentation limits clinicians' ability to review glucose patterns during routine visits, impedes care coordination across providers, and constrains population health initiatives that depend on integrated data for risk stratification and outcome measurement. Patients frequently struggle to share their device data across care settings or to exercise meaningful control over how their information is used. Meaningful progress has been made. Since the 21st Century Cures Act in 2016 and the introduction of the iCoDE standard in 2022, the major manufacturers and aggregators have moved toward integration, and as this paper's data dictionary shows, they now largely agree on how the core CGM metrics are defined. The technical capability to integrate CGM data increasingly exists. What remains is not primarily a technical problem; the barriers are financial, operational, and contractual, and the federal rules that would compel integration do not yet reach the device platforms where the data live.

The federal regulatory landscape has not kept pace with the growth of medical device data. While the Health Insurance Portability and Accountability Act (HIPAA) establishes patient access rights to protected health information, and the Health Information Technology for Economic and Clinical Health (HITECH) Act strengthened those rights,[4] the 21st Century Cures Act prohibits information blocking by defined actors: healthcare providers, health information networks and exchanges, and health IT developers of certified health IT.[5] CGM cloud portals are typically not certified health IT and therefore fall outside the interoperability and information-blocking provisions that govern EHR vendors. The United States Core Data for Interoperability (USCDI) standards and the Trusted Exchange Framework and Common Agreement (TEFCA) offer potential pathways for CGM data inclusion, but neither currently mandates device data integration.[6,7] Recent federal attention to this gap, including the May 2025 CMS/ASTP-ONC Request for Information on the Health Technology Ecosystem and the HTI-5 Proposed Rule released in late 2025, reflects both recognition of the problem and an emerging policy window for reform.[8,9]

Advancing CGM data policy requires navigating a complex landscape of interests. Device manufacturers have legitimate interests in protecting proprietary algorithms and managing liability exposure. Data aggregators and EHR vendors face technical and contractual challenges to integration. Health systems face those as well, but their central barrier is financial: the cost of integrations and subscriptions, without payment models that let them recoup the investment. Patients and advocates seek transparency, control, and equitable access. Payers set the reimbursement and coverage policies that determine whether integrated CGM data can be delivered sustainably under both fee-for-service and value-based care

arrangements, and those policies are still evolving. No durable policy solution can emerge without structured dialogue among these groups and genuine consensus on shared principles.

In 2023, the Rising T1DE Alliance proposed to undertake a cross-sector initiative to address CGM data policy gaps. This white paper is the culmination of that process and describes our approach to convening diverse participants, summarizing the policy landscape, and eliciting patient and caregiver perspectives broadly. Through a collaborative and iterative year-long process, our crosscutting working group articulated six policy recommendations grounded in existing statutory and regulatory authorities. Our aim is both to advance this particular policy domain and to offer a replicable model for patient-centered, consensus-driven health technology policy development.

2. Policy Landscape

Medical device data sits at the intersection of multiple federal regulatory regimes, none of which fully covers it. Understanding why CGM data remains difficult to access, share, and integrate requires understanding both the foundations of U.S. health information policy and the more recent regulatory activity reshaping the landscape. This section traces that arc.

2.1 The Federal Foundation

HIPAA and HITECH: Patient Access Rights

The Health Insurance Portability and Accountability Act (1996) established the foundational framework for protected health information, including patient rights to access their own data held by covered entities. The HITECH Act of 2009, particularly Section 13405(e), strengthened patient access by requiring that electronic health information be made available to patients in electronic form, including the right to direct that information to a third party of the patient's choosing.[4] These provisions apply when CGM data is held by a covered entity (such as a healthcare provider) or its business associate. They do not extend directly to CGM cloud portals and aggregator platforms when those operate outside the covered-entity relationship. A further complication sits alongside the regulatory one. If integration agreements between device platforms and health systems restrict onward sharing of the data they cover, then a patient right and a contractual term can point in different directions even where the data has reached a covered entity. This is one of the recurring friction points that Recommendation 5 addresses.

21st Century Cures Act and Information Blocking

The 21st Century Cures Act (2016), specifically Section 4004 and implementing regulations at 45 CFR Part 171, prohibits information blocking by healthcare providers, certified health IT developers, and health information networks. Information blocking is defined as a practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI), unless a defined exception applies. Once CGM data is held by a covered actor as EHI (e.g., incorporated into the EHR), patients are entitled to timely, electronic access to it, and contractual terms, cost structures, or technical design cannot functionally restrict that access. Exceptions are limited and narrowly defined in regulation, covering circumstances such as preventing patient harm, protecting privacy and security, and genuine technical infeasibility.[5] Critically, however, CGM manufacturers and device data platform operators do not develop or offer certified health IT and so fall outside that actor category, even though the data they hold may be clinically important and may ultimately flow into systems operated by covered actors.

ONC Certification, USCDI, and TEFCA

The Office of the National Coordinator for Health Information Technology (ONC), titled the Assistant Secretary for Technology Policy/ONC (ASTP/ONC) from 2024 until early 2026, operates the Health IT Certification Program. Certification is the mechanism that turns interoperability standards into practice. To be certified, health information technology, such as an electronic health record system, must demonstrate that it meets defined functional and technical requirements, including standardized application

programming interfaces (APIs) and data formats. This matters because certification is tied to participation in federal programs, so most hospitals and clinicians use certified systems and the requirements ONC sets propagate across the field. Certification also defines an important boundary for ONC's regulation of technology developers; Device platform operators that do not meet the definition of "health IT developer of certified health IT" are not brought within the framework merely because they develop health technology.

Within that program, the United States Core Data for Interoperability (USCDI) defines the baseline set of data classes and elements that certified systems must be able to exchange; it functions as the common vocabulary of interoperable health data. USCDI is versioned and expands over time as new data types are adopted. Certified systems are currently required to support USCDI v3; no published version, through v7 (July 2026), explicitly includes CGM data elements, a central gap this paper addresses.[29] Until CGM metrics are named in USCDI, certified systems are not required to carry them in a standardized way, although patient-generated health data is referenced in current guidance.

The Trusted Exchange Framework and Common Agreement (TEFCA) operates one layer up, establishing a nationwide network of networks through which qualified health information networks exchange data under a single common agreement, so that a query placed in one network can reach records held in another. TEFCA reached 500 million records exchanged in February 2026, demonstrating that the national exchange rails are operational.[6,7] In principle it could carry CGM data, but it does not yet mandate it, and patient-generated data are only beginning to be addressed within it.

FDA and Device-Level Interoperability

The Food and Drug Administration regulates CGM systems as medical devices, and its framework governs interoperability at the device level, distinct from the data-exchange questions ONC addresses. In 2018, through a De Novo request from Dexcom, the FDA created a new device category, the integrated continuous glucose monitoring (iCGM) system, and classified it as a moderate-risk class II device subject to special controls.[23] The significance for interoperability is twofold. First, the iCGM pathway is explicitly designed around integration: an iCGM is authorized to communicate with other compatible devices, such as automated insulin delivery systems and insulin pumps, and future systems that meet the special controls can reach market through the more streamlined 510(k) pathway. Second, the special controls address data security directly, identifying insecure data transmission as a risk that manufacturers must mitigate. The FDA framework therefore establishes interoperability and security expectations for how devices connect to one another; it does not, however, govern how CGM data flows into the electronic health record or to patients and third parties, which remains the province of the ONC and CMS authorities described below.

2.2 The Recent Regulatory Wave

Most recent federal activity on health data interoperability has come through a series of ONC rulemakings known by the shorthand HTI, for Health Data, Technology, and Interoperability. ONC issues these rules through the standard federal notice-and-comment process: it publishes a proposed rule in the Federal Register, accepts public comment for a defined period, and then issues a final rule that carries the force of regulation. Each HTI rule updates the ONC Health IT Certification Program, the set of functional and

technical requirements that electronic health record systems must meet to be certified. Because most hospitals and clinicians use certified systems, these rules shape, indirectly but powerfully, what health data can be exchanged and how. The sequence matters for CGM because it establishes the technical direction, FHIR-based APIs, that any future device-data integration would most plausibly follow.

HTI-1 through HTI-4: The API-Forward Direction

Beginning with the HTI-1 final rule in early 2024 and continuing through the HTI-2 and HTI-4 rulemakings, ONC has progressively established FHIR-based application programming interfaces (APIs) as the expected technical foundation for health information exchange. FHIR, Fast Healthcare Interoperability Resources, is a modern data exchange standard that allows different systems to request and share discrete data elements in a consistent format. These rules require certified systems to expose patient-access APIs aligned to the US Core FHIR Implementation Guides and to support standardized authorization workflows, so that a patient or an authorized application can retrieve data programmatically rather than through manual export. The cumulative effect has been to make API-based exchange the default expectation for certified health IT, and to make USCDI the reference for which data elements those APIs must carry.

HTI-5: Deregulation and the Safety Tradeoff

Status: HTI-5 comment period closed February 27, 2026; final rule pending.

The Rising T1DE Alliance submitted formal comments on February 26, 2026 (Appendix E).

The HTI-5 proposed rule, published in the Federal Register on December 29, 2025, would consolidate the API-first direction while sharply reducing the certification burden on developers. As proposed, it would remove 34 and revise 7 of the 60 current certification criteria, modernize the FHIR-based exchange requirements, and change several information-blocking provisions, including removal of the TEFCA Manner Exception.[20] ONC frames the rule as a deregulatory effort to eliminate duplicative requirements and redirect the field toward AI-enabled interoperability. The direction is defensible, but the proposal is not without risk, and the Rising T1DE Alliance said so in its public comments.[9] Removing or replacing certification criteria wholesale can weaken the baseline assurances that health systems currently rely on: audit logging, authentication, encryption, and API performance transparency. When those assurances are relaxed at the certification level, the safety and operational burden does not disappear; it shifts onto the healthcare organizations that must still make device and patient data flow safely. RTA's comments therefore supported the API-forward direction while urging ONC to retain, or clearly replace, those baseline expectations rather than simply remove them. As proposed, HTI-5 applies to certified health IT and not directly to device manufacturers, so the CGM data gap persists in the proposed rule.

HTI-6: A Possible Opening for Device and Wearable Data

The next rule in the sequence, HTI-6, has not been proposed, but ONC indicated in connection with the HTI-5 rulemaking[20,30] that an HTI-6 proposed rule could follow later in 2026 and could, for the first time, require electronic health records to support data exchange with wearable devices. Timing and scope remain uncertain, and no proposal text exists. Even so, the prospect matters, because it suggests that the device-data gap left open by HTI-5 may finally begin to close, and because it opens a window in which interested parties can help shape how wearable and patient-generated data are treated before

requirements are fixed in regulation. Released as the HTI-6 conversation takes shape, this white paper is intended in part to inform those choices.

ONC and CMS: Complementary Paths to Interoperability

The regulatory picture described above shifted during 2026, making it increasingly important to understand which federal entities hold which policy levers. Two changes matter. First, the office that had been titled the Assistant Secretary for Technology Policy/ONC (ASTP/ONC) from 2024 reverted to its original name, the Office of the National Coordinator for Health Information Technology (ONC), effective April 1, 2026.[21] Second, CMS established a new Office of Health Technology and Products, effective June 9, 2026, consolidating its standards, interoperability, product-development, and digital-service functions under a single FHIR-API-first office that coordinates with ONC.[22] The result is that ONC and CMS now play distinct but complementary roles in federal interoperability policy. ONC oversees certification, standards, and the information-blocking framework. CMS, through its new office, oversees the interoperability expectations built into the programs CMS runs, from Medicare and Medicaid to the CMS Interoperability Framework described in the next section. For CGM data, this distinction is consequential because CGM platforms generally fall outside the scope of ONC's certification program. The CMS program side, by contrast, is a lever that does not depend on health IT certification: it can set expectations through program participation and payment rather than through certification. This dual structure offers two complementary paths forward, and the recommendations in this paper are designed to work with both: program alignment and voluntary consensus through CMS, and standards and certification through ONC.

2.3 The CMS Interoperability Framework

In July 2025, following a spring 2025 Request for Information on the health technology ecosystem, the Centers for Medicare & Medicaid Services released the CMS Interoperability Framework. The Framework is a voluntary blueprint comprising 26 criteria across five domains: patient access and empowerment; provider access and delegation; data availability and standards (including USCDI v3 and FHIR/US Core APIs by July 4, 2026); network connectivity and transparency; and identity, security, and trust (including IAL2/AAL2 digital credentials and HITRUST-equivalent security validation). At launch, more than 60 organizations pledged to align with the Framework and showcase real-world implementations by early 2026.[10]

For CGM data, the Framework functions as a design target and market signal rather than a stand-alone regulation. CMS explicitly notes that the Framework is not intended to create new regulatory burdens but to build alignment on top of existing laws, including HIPAA, the 21st Century Cures Act information-blocking provisions, TEFCA, and the CMS Interoperability and Prior Authorization final rule. The recommendations in Section 6 of this paper are designed to operationalize the Framework for device-derived data. A detailed alignment between our six recommendations and specific CMS Framework criteria appears in Appendix C.

2.4 Reimbursement and Care-Delivery Context

Policy on data access is shaped by, and shapes, how care is paid for. Reimbursement policy has supported CGM adoption through two related pathways: coverage of the devices themselves and payment for the

clinical work of interpreting their data. CPT code 95251, which allows clinicians to bill for analysis, interpretation, and reporting of CGM data, was established in 2006 and can be billed on as little as 72 hours of data. Medicare's 2017 CGM coverage expansion subsequently accelerated access to the devices themselves and was followed by uneven Medicaid and commercial uptake. Together, these policies helped establish both access to CGM technology and a mechanism for incorporating its data into individual patient care.

As diabetes care has become more continuous and data-driven, reimbursement has expanded beyond CGM-specific interpretation to broader remote monitoring and chronic-care services. The 2026 Physician Fee Schedule introduced significant changes to remote patient monitoring (RPM) reimbursement, including two-to-fifteen-day windows and shorter management codes, changing how device-generated data can support reimbursable clinical workflows.[24] These new short-window RPM codes sit alongside older RPM codes that require sixteen or more days of data in a period, CGM-specific interpretation codes that can be billed on as little as seventy-two hours of data, and chronic care management codes that are often layered onto RPM but demand substantial care-coordination infrastructure.[24, 25] Coverage also diverges across Medicare, Medicaid, and commercial payers, and it can be volatile. In late 2025, a major commercial payer moved to end RPM coverage for diabetes and other chronic conditions as insufficiently supported by evidence, then paused the change after legal and clinical pushback, leaving its policy unresolved.[26, 27] For clinicians and health systems weighing whether to build data-driven diabetes programs, fragmented coding and unstable coverage are themselves a barrier, independent of the technical access questions this paper addresses.

At the same time, CMS payment policy is moving toward more clinically integrated and accountable use of remotely generated data. Value-based care models, including those operated by the CMS Innovation Center, increasingly rely on device and clinical data for population health and risk stratification. In the proposed CY2027 Physician Fee Schedule, released in July 2026, CMS proposed to pay for remote monitoring only when the services are furnished by clinical staff employed by the billing practice, rather than outsourced to third-party vendors, citing Office of Inspector General findings that a large share of monitored patients never received all of the required components of the service.[28] The proposal is not final (public comments closed September 2026), but its direction is clear. Reimbursement is shifting toward monitoring that is clinically integrated and accountable, not billing-driven. In modern, data-driven diabetes care, CGM data are no longer ancillary; they are core clinical infrastructure. Yet current reimbursement, whether through fee-for-service CGM interpretation and RPM or emerging value-based-care arrangements, may still be insufficient to sustain the staffing and operational effort required to deliver proactive, data-driven diabetes care at scale. Sustaining this model over the long run will likely require stronger reimbursement pathways to support these services.

Early implementation experience illustrates both the promise and the fragility of this model. A pediatric specialty value-based care program for type 1 diabetes at Children's Mercy Kansas City paired guaranteed infrastructure funding with performance-dependent payments tied to clinical quality and utilization measures, supported by a population health approach in which CGM and electronic health record data were integrated to enable weekly population review, risk stratification, and proactive outreach through remote monitoring and care management. Across the attributed population, this approach was associated

with sustained improvement in glycemic control and reduced acute care utilization over the observation period; population median HbA1c and the proportion of patients above the high-risk threshold both declined, as did inpatient and emergency department utilization. The program is described in a submitted manuscript that, to the authors' knowledge, represents the first formal report of a pediatric specialty value-based care program for type 1 diabetes in the United States.[12] Two features of that experience bear directly on data policy. First, the care model depended on the ability to ingest CGM data into a population health platform, which required contracting with data aggregators and direct manufacturer application programming interface (API) access; the same access barriers this paper addresses were rate-limiting in practice. Second, the model was financially viable only because infrastructure funding was paired with performance-based payments; neither fee-for-service RPM nor performance payments alone would likely have sustained the between-visit staffing and analytic effort the model required. The lesson is not that this particular program is a template, but that streamlined data access and adequately structured reimbursement are jointly necessary conditions for data-driven diabetes care to move from well-resourced early adopters to routine practice.

This points to a broader opportunity, and an open invitation. Making continuous monitoring a durable part of diabetes care infrastructure, rather than a capability sustained only by well-resourced early adopters, will take more than technical access. It will require the health-economics evidence to support updating professional care guidelines, such as the ADA Standards of Care, so that remote and continuous monitoring are recognized as core to the management of insulin-dependent diabetes, paired with reimbursement adequate to sustain that work under both fee-for-service and value-based care. No single organization can build that evidence and alignment alone; it will take payers, quality organizations, clinicians, and advocates working toward shared goals. This paper offers the concept and a starting point, and invites the parties who would need to be part of that effort to help define and pursue it, in the same spirit as its themes on patient consent and on adopting new clinical quality metrics.

2.5 State-Level Activity

Several states have begun to legislate digital health data exchange and interoperability beyond federal baselines. California's AB 133 (2021) requires health care providers, health plans, and other covered entities to exchange health information in real time under the state's Data Exchange Framework.[31] New York requires health care facilities using certified electronic health record technology to connect to its Statewide Health Information Network (SHIN-NY) by regulation and has continued to expand its interoperability requirements.[32] State activity is fragmentary, but it can create pressure for industry change where federal requirements are absent.

2.6 Voluntary and Non-governmental Frameworks

Not all of the standardization work relevant to CGM data has come from government. Several voluntary, consensus-driven efforts have developed much of the technical and operational groundwork that policy can build on, rather than duplicate. These frameworks matter for two reasons: they show that the technical path to CGM-EHR integration is already well defined, and they offer ready-made reference points that policy can adopt or encourage rather than reinvent.

iCoDE (Integration of Continuous Glucose Monitoring Data into the Electronic Health Record). Convened by the Diabetes Technology Society, the iCoDE project brought together clinicians, patients, data aggregators, manufacturers, informaticists, attorneys, and cybersecurity experts to develop consensus standards for CGM-EHR integration. The *2022 iCoDE Report: CGM-EHR Integration Standards and Recommendations*, organized across six working groups spanning data standards, account linkage, integration and interoperability, analytics and visualization, clinical workflows, and business models, remains the most comprehensive standards-based guidance available for organizations pursuing CGM-EHR integration. A successor effort, iCoDE-2, extended the same approach to insulin dosing and other connected drug-delivery device data.[33] iCoDE is the reference framework for the CGM data dictionary developed in this paper (Appendix A) and is cited throughout the recommendations as the preferred alignment target.

HL7 FHIR Continuous Glucose Monitoring Implementation Guide. Building on requirements first developed in the Argonaut Project, with input from patients, providers, CGM device vendors, application developers, and EHR systems, and subsequently advanced with the HL7 Orders and Observations Work Group, the HL7 CGM Implementation Guide defines a standardized method for submitting CGM data into the EHR using FHIR. It specifies how summary metrics, including glucose management indicator, time in ranges, mean glucose, and coefficient of variation, as well as raw sensor readings, are structured and exchanged; it uses SMART on FHIR for authorization and supports both scheduled standing orders and on-demand requests. It also defines a lighter-weight sharing mechanism, based on SMART Health Links, for situations where full system-to-system integration is not feasible, such as sharing with schools or temporary caregivers. The guide has reached STU1, meaning it is ready for real-world implementation while remaining open to feedback and future updates. Together with iCoDE, it means the technical specifications for moving CGM data into the EHR largely exist; the barrier is adoption, not invention.[13]

IEEE 2621 (Wireless Diabetes Device Security). The IEEE 2621 series, developed jointly by IEEE and UL, provides cybersecurity standards for connected diabetes devices, including CGMs, insulin pumps, smart insulin pens, and automated insulin delivery systems. The series defines a security assurance evaluation framework, information security requirements for connected diabetes solutions, and guidance on the use of mobile devices in diabetes control contexts. IEEE 2621 does not govern data exchange or format; rather, it addresses the security and assurance layer on which trustworthy data sharing depends. It is relevant to this paper because patient trust and safe interoperability require that the devices and platforms exchanging CGM data meet a consistent security baseline.[14]

Ambulatory Glucose Profile (AGP). Developed through an expert consensus led by the International Diabetes Center and published in 2013, the Ambulatory Glucose Profile established a single standardized report format for CGM data: a consistent set of glycemic metrics with a consistent visual presentation. It has since been adopted broadly across CGM and aggregator platforms; the International Diabetes Center maintains the specification, currently at version 5.0, and CGM manufacturers and aggregators license it for integration into their platforms. AGP occupies a distinct layer from the data standards described below: AGP standardizes how CGM metrics are presented and interpreted at the point of care, while iCoDE, LOINC and USCDI standardize how the underlying data are defined, coded and exchanged. The two are

complementary, and contributors to the CGM Data Dictionary in Appendix A cite the IDC AGP v5.0 definitions directly for specific fields.[19]

Quality measurement and NCQA. Quality measurement is emerging as a distinct lever for CGM data standardization. The glucose management indicator (GMI),[17] derived from CGM data, is currently part of NCQA quality measurement in both the Healthcare Effectiveness Data and Information Set (HEDIS) and the Diabetes Recognition Program, alongside a companion indicator of whether a patient uses a CGM.[18] Additional CGM-derived metrics, such as time in range and time of wear, have been discussed as possible future measures but are not part of the current measure set. Because quality measures shape how health systems and payers prioritize data capture, the recognition of CGM-derived metrics in quality frameworks creates a practical, non-regulatory incentive for consistent data definitions and reliable data flow; conversely, standardized definitions and calculation methods across manufacturers and aggregators would reduce a barrier to any future expansion of CGM-based quality measures. This connection is developed further in Recommendation 6.

2.7 The Gap That Remains

Taken together, these regulatory authorities do most of the work needed for medical device data while leaving one underlying problem unresolved. The United States has fairly robust health data policies, but today they apply to CGM data and CGM data platforms inconsistently. Their application depends on the entity holding or exchanging the data and the regulatory role that entity occupies. HIPAA patient-access rights apply when CGM data are maintained by a covered entity or business associate; the information-blocking framework applies to covered actors, but CGM manufacturers and device data platforms do not fall within that definition. USCDI does not yet name CGM data elements; TEFCA enables exchange but does not require device-data participation; HTI-5 reinforces API-first exchange without directly resolving the device platform gap; and the CMS Interoperability Framework covers most of what is needed but is voluntary. The task is to find a meaningful way for medical device data systems to operate under the same or similar rules, whether through new categories of certified health IT, new policy, or clarifications that extend existing requirements to those systems. Policy momentum, coverage and payment evolution, and care-delivery incentives converge to make this an unusually favorable moment for that work. The remainder of this paper describes how participants came together to define what it should look like, and what should happen next.

3. Methods and Engagement Process

The Rising T1DE Alliance designed a mixed-methods, engagement-driven policy development process spanning June 2025 through October 2026. The initiative integrated regulatory analysis, formal federal policy engagement, iterative cross-sector convenings, and structured patient and advocate engagement to build consensus on actionable policy recommendations. The work is grounded in participatory policy design principles, ensuring that patient perspectives inform every phase rather than serving merely as validation of expert-derived proposals.

3.1 Regulatory Landscape Review

We conducted a structured review of federal policies relevant to CGM data access and interoperability, including HIPAA privacy and access provisions, HITECH Act patient access rights under Section 13405(e), 21st Century Cures Act information-blocking prohibitions under Section 4004, the ONC Health IT Certification Program, USCDI, TEFCA, the HTI-1 through HTI-5 rulemakings, the CMS Interoperability Framework, and emerging signals around HTI-6. For each regulatory mechanism we examined how it applies, or fails to apply, to medical device data platforms. The review also incorporated grey literature including white papers, advocacy reports, and ONC guidance documents. Findings from this review are summarized in **Section 2** and identify the existing authority anchoring each recommendation in **Section 6**.

3.2 Federal Regulatory Policy Engagement

In May 2025, CMS and ONC (then ASTP/ONC) released a Request for Information titled *Health Technology Ecosystem*. The Rising T1DE Alliance submitted formal comments advocating that medical device platforms be held to equivalent standards as certified health IT systems, with specific recommendations for extending patient access requirements, USCDI compliance, and information-blocking prohibitions to device data portals (Appendix D). In February 2026, RTA submitted public comments on the HTI-5 Proposed Rule supporting its API-forward direction while urging ONC to retain or clearly replace baseline expectations for audit logging, authentication and authorization, encryption, and API performance transparency (Appendix E). Both submissions served as public statements of RTA's policy positions and as inputs to the working group process.

To clarify policy objectives, understand participant interests, and identify potential concerns, we conducted individual meetings with participants before and after each Working Group Meeting. One-on-one engagements with all working group participants continued throughout the initiative, supporting recruiting, onboarding, and post-session feedback, and shaping the design of implementation workstreams.

3.3 Cross-Sector Working Group Meetings

Once the participants were established, we structured the Working Group process as five Working Group Meetings spanning June 2025 to August 2026, complemented by a dedicated orientation session for patients, caregivers, and advocacy organization representatives in September 2025. The first Working

Group Meeting convened device manufacturers and data aggregators only, and the orientation session convened the patient community only; this allowed us to provide targeted education to each group, build shared understanding, and surface priorities before bringing the groups together. From the second Working Group Meeting (November 2025) onward, all participants met together, with NCQA joining at that meeting for the first time. Sessions were conducted virtually for ninety minutes. Perspectives were captured without attribution to individuals or organizations, and attribution is permitted only with explicit consent.

Meeting	Date	Focus
WG1	June 2025 (ADA, Chicago)	Industry kickoff: manufacturers and aggregators only; established initial joint policy framework
Orientation	September 2025	Dedicated patient, caregiver, and advocacy orientation; no industry participants; built shared understanding and surfaced priorities before integration into cross-sector sessions
WG2	November 2025	Expanded participation: patients, advocacy organizations, and NCQA joined; deep dives on patient access and interoperability
WG3	February 2026	Mid-course review: refined recommendations and patient survey 1 feedback; introduced implementation pathways framing
WG4	May 2026	Patient survey 2 findings; recommendations convergence; deep dive on anti-information blocking; white paper draft preview
WG5	August 2026	Final review and sign-off on consensus recommendations and appendices

The Working Group was intentionally structured around the stakeholders most directly affected by the policy questions under consideration: CGM manufacturers and data aggregators, whose technical and business practices would be most directly affected by changes in data-access and interoperability requirements, and patients and caregivers, whose ability to access, share, and benefit from these data is the ultimate focus of this work. Payers and health systems were not convened as distinct participant groups in this phase. Their roles are important but downstream of the foundational question of whether CGM data are available in a form that can support sharing, clinical integration, and new models of care.

Payer perspectives entered the work through the policy landscape review, through quality-organization participation, and through the project team's direct experience developing and operating the pediatric specialty value-based care program described in **Section 2.4**, in which remote patient monitoring and CGM data integration were central to the care model. Direct payer engagement remains a limitation of this phase and a priority for future work, particularly in defining the evidence needed to support sustainable reimbursement for remote monitoring and data-enabled diabetes care. Clinical and health-system implementation perspectives were represented through the experiences of project team members and through the broader body of clinical guidance and interoperability work, including iCoDE, that informed the recommendations. Future phases should include more direct engagement with both payers and health systems as the work moves from data-access policy toward implementation, financing, and care delivery.

3.4 Patient and Advocate Engagement

Patient-centered design required deliberate attention to engagement structure. Prior to integrating patients into cross-sector sessions with industry, we conducted a dedicated overview session in late September 2025 with patients, caregivers, and advocacy organization representatives, with no industry participants present. This design choice ensured community members could build foundational understanding of the technical and policy issues, articulate their priorities, and identify concerns without being overshadowed by other participants. We conducted individual recruitment and onboarding conversations with patients and advocacy organization leaders.

To complement the perspectives of those participating directly in the Working Group, we conducted a series of patient and caregiver surveys designed to bring broader community perspectives into the policy-development process and inform successive Working Group discussions. Patients and advocacy partners were actively engaged in survey design. For each survey, patient and advocacy representatives reviewed and signed off on the instrument before it was fielded. After fielding, the same group previewed survey findings ahead of the broader working group and helped interpret what the results meant and decide which findings to surface in the time-constrained cross-sector sessions. Debriefs were held in February 2026 for Survey 1, in May 2026 for Survey 2, and in August 2026 for Survey 3; Survey 3 fielding continued after that debrief as additional invitations were released. This two-touch cycle, sign-off before fielding and shaping of interpretation before dissemination, kept patient and advocacy voice central to both what was asked and how the answers were understood. Survey methods and findings are described in **Section 4.1**.

3.5 Implementation Workstreams

Two parallel implementation workstreams run alongside the working group process and feed directly into the white paper appendices:

- **CGM Data Dictionary.** A shared reference of standardized CGM metrics anchored in the iCoDE Core Dataset, with manufacturer alignment status tracked for each metric. The dictionary appears in Appendix A.
- **Shared Contracting Principles.** A set of guiding principles addressing recurring contracting friction points across EHR integration permissions, multi-device consent portability, data granularity, and downstream sharing restrictions. The principles appear in Appendix B.

3.6 Analysis and Synthesis

Each evidence stream was analyzed on its own terms before synthesis. Working group discussions were recorded, transcribed, and analyzed thematically, with positions tracked at the level of participant groups consistent with the attribution approach described above. Survey data were analyzed descriptively, wave by wave; because the three waves were fielded as independent samples and responses were deliberately not linked to screener records to preserve anonymity, results are reported for each wave's full sample, with panel characteristics described in aggregate from the screener, and responses were screened for data quality before analysis. The data dictionary was developed through structured comparison of contributor

submissions against the iCoDE Core Dataset, with alignment status confirmed by each contributor, and the shared contracting principles were derived thematically from individual participant interviews. The recommendations in **Section 6** draw on convergence across these streams where it emerged; where perspectives diverged, the divergence is reported in the **Section 5** findings. The recommendations themselves are the authors' positions: informed by every stream, strengthened by consensus where it existed, and not contingent on unanimity among participants. Open discussion questions within each recommendation identify the implementation choices, of mechanism, sequence, and threshold, where continued participant input will shape how each position is put into practice.

3.7 Limitations and Exclusions

The scope of this process was deliberately bounded. Several groups whose perspectives matter to CGM data policy were not part of the working group, and naming those choices here is meant to make the basis of the recommendations legible rather than to claim completeness.

Clinicians were not systematically recruited. Some participants happen to practice clinically, and their perspective informed the discussion incidentally; clinicians were not, however, convened as a constituency. This was deliberate. The clinical requirements for CGM data in practice are already well characterized through the iCoDE standards, international consensus work on CGM metrics, and a substantial peer-reviewed literature. The gap this process set out to close lay between patients and the organizations that hold their data, and that is where the convening effort was concentrated.

EHR vendors did not participate. Electronic health record vendors sit on the receiving end of most of the exchange this paper contemplates, and several recommendations, particularly those concerning interoperability standards and information blocking, have direct implications for them. Their absence means that the operational cost and sequencing of the changes proposed here have been assessed largely from the device and platform side. Recommendations 2 and 4 would benefit from vendor input at the implementation stage.

Payers did not participate. Coverage and payment policy determine whether integrated CGM data can be delivered sustainably, and **Section 2** describes that landscape from the public record rather than from direct engagement. The paper therefore describes payment as context and constraint; it does not propose payment policy, and the recommendations should not be read as having been tested against payer feasibility.

Survey limitations are addressed where the survey findings appear. The composition of the respondent panel, its recruitment, and the resulting limits on generalizability are described in **Section 4** alongside the findings themselves, and are not restated here.

None of these exclusions are fixed. Each names a constituency whose participation would strengthen the next phase of this work.

4. Patient and Caregiver Perspectives

Patient and caregiver perspectives were incorporated directly into the development of the recommendations. As part of this initiative we conducted three online surveys of people living with type 1 diabetes and their caregivers, fielded in sequence between December 2025 and September 2026 and timed to inform successive Working Group Meetings. This section describes what we asked, who responded, and what we found, survey by survey, and closes with the lessons that hold across all three.

4.1 Survey Methods

Participants were recruited into a standing survey panel through a public screening questionnaire, distributed with the support of the T1D Exchange, which shared the screener through its emails, portals, and newsletters. Because the screener was distributed openly rather than to a closed list, the total number of people who saw the invitation is not known. The screener closed after 455 completed responses. Screener respondents were then filtered to those who were eighteen or older, who had type 1 diabetes, cared for someone with type 1 diabetes, or worked with a diabetes organization, and who indicated interest in joining the survey panel.

Each survey was administered electronically through REDCap and kept open until it reached 100 completed responses, with invitations released in waves so that completion could be monitored. Survey 1 invited 152 panel members, drawn in screener response order on the recommendation of our recruiting partners as the fairest available method, and reached 100 completed responses. Following Working Group discussion of the need to broaden representation, Survey 2 returned to the screener and prioritized invitations to panel members who had identified a race or ethnicity other than White; because that group alone was not large enough to reach the target, Survey 1 invitees were also invited, for 126 invitations and 100 completed responses. Survey 3 re-invited the same 126 panel members and added 67 extension invitations in three batches, for 193 invitations total.

All survey records underwent data-quality and eligibility review before analysis. Records that did not meet those criteria, including non-independent submissions identified in Surveys 2 and 3, were excluded. Final analytic samples were 100 respondents for Survey 1, 46 for Survey 2, and 92 for Survey 3. The engagement cycle around each survey, including instrument sign-off before fielding and interpretive debriefs afterwards, is described in **Section 3.4**.

A post-fielding data-quality review identified coordinated, non-independent submissions affecting survey waves 2 and 3, traced to fabricated identities enrolled through the open recruitment screener. Records from the 54 identities responsible, identified by their presence in documented bulk-completion bursts in both waves, were excluded prior to analysis; all findings reflect verified respondents only. Wave 1 was unaffected. Enrollment verification, monitored invitation release, and honoraria release following data-quality review have been adopted for all subsequent fielding. All figures reported here were finalized on the closed, verified sample.

How to read these results

The three surveys drew on the same recruitment networks but were fielded as independent samples rather than as a longitudinal cohort. Although some respondents participated in more than one survey, the surveys were not designed to track individuals over time. Findings are therefore reported survey by survey, and differences between waves should not be interpreted as change over time within a single group.

4.2 Who Responded

Participant characteristics are summarized in two tables. Demographic characteristics, including gender, race, ethnicity, and insurance, were collected through the initial screening questionnaire to characterize the survey panel and inform recruitment. These questions were not repeated in each survey, and survey responses were not linked to individual screening records. **Table 1** describes the characteristics of all panel members who contributed to at least one survey, rather than the respondents to any individual survey. **Table 2** presents characteristics collected within each survey, including respondent role, care setting, CGM use, diabetes duration, and use of automated insulin delivery.

Table 1. Screener characteristics of panel members who contributed to at least one survey (n=147).

Characteristic	n (%)
CGM use, more than 3 years	132 (90%)
CGM use, 1 to 3 years	14 (10%)
Prior diabetes advocacy or policy participation	42 (29%)
Gender: woman	88 (60%)
Gender: man	57 (39%)
Gender: other or prefer not to say	2 (1%)
Insurance: private or employer-sponsored	85 (58%)
Insurance: public (Medicaid or Medicare)	58 (39%)
Insurance: other, not sure, or uninsured	4 (3%)
Race or ethnicity: White	136 (93%)
Race or ethnicity: Hispanic or Latino	9 (6%)
Another race or ethnicity, or preferred not to say	12 (8%)
Zip code provided	139 (95%)

Demographic characteristics were collected through the screening questionnaire and are reported in aggregate; they cannot be linked to individual survey responses. Race and ethnicity were asked as a select-all question, so percentages within that block sum to more than 100%.

Table 2. Characteristics of respondents in each survey wave. Characteristics are reported per wave and are not linked across waves or to screener records.

Characteristic	Survey 1 (n=100)	Survey 2 (n=46)	Survey 3 (n=92)
Field period	Dec 2025 - Feb 2026	Mar - Apr 2026	Jul - Sep 2026
Panel members invited	152	126	193
Completed responses	100 (none excluded)	46 verified of 100	92 verified of 149
Respondent type			
Person living with T1D	100%	100%	96%
Caregiver / parent / partner	0%	0%	4%
Care setting			
Adult endocrinology	91%	91%	83%
Primary care / PCP	14%	11%	13%
Telehealth / virtual	5%	7%	3%
Community / rural clinic	0%	0%	2%
Pediatric endocrinology	2%	0%	5%
CGM brand			
Dexcom	85%	76%	77%
Medtronic / MiniMed	8%	15%	12%
Abbott / FreeStyle Libre	5%	11%	11%
Eversense	1%	0%	0%
T1D duration over 20 years	72%	Not asked	Not asked
Uses an AID system	71%	Not asked	Not asked
Completed the prior survey	Not applicable	67%	32% Survey 2; 37% Survey 1

Care setting was asked as a select-all question in all three surveys, so percentages within that block sum to more than 100. CGM brand was asked as a single-choice question in Survey 1, as a select-all question in Survey 2, and in Survey 3 as a single choice of the brand used most often; the Survey 2 column is therefore not directly comparable with the other two, and one Survey 2 respondent selected two brands.

Important caveat on representativeness

These findings reflect feedback from a highly engaged participant group recruited through patient advocacy and type 1 diabetes research networks. Respondents skew heavily toward long-duration type 1 diabetes, adult endocrinology care, and automated insulin delivery use. Two limitations bear directly on interpretation. First, the screened panel was predominantly White (93 percent), with more women than men (60 versus 39 percent); the Working Group identified this early, and Survey 2 responded by prioritizing invitations to panel members who had identified an ethnicity other than White, although the number of such panel members available was small. Second, because survey responses were deliberately not linked to invitation records in order to preserve anonymity, the racial, ethnic, and gender composition of the people who responded to any individual survey is not known; it can be described only at the level of the verified panel reported in Table 1, and age was not collected beyond the eighteen-or-older eligibility screen. These results should therefore not be read as representative of all people living with diabetes, particularly individuals from communities underrepresented in CGM use or in research participation. Broadening the range of patient experiences reflected, including through targeted recruitment via community and rural clinics, is a priority for future phases of this work.

4.3 Survey 1: Access, Coordination, and the Limits of Data Use

What we asked. Survey 1 was fielded from December 2025 through February 2026 and comprised 29 questions across six sections: respondent context and diabetes technology; access to their own CGM data; care coordination across providers; use of CGM data by providers and academic researchers; health insurance plans, coverage, and data use; and a ranking of top priorities. Results were presented at Working Group Meeting 3 and informed the design of the recommendations.

What we found. For patients, seeing their own data is largely solved; getting it to everyone who needs it is not. Ninety percent of respondents found it easy or very easy to see their own CGM data. Sharing that data with more than one provider at once was markedly harder: only 55 percent found it easy, while 28 percent had not tried or were unsure how.

Care team visibility is assumed more than verified. Seventy-nine percent were very or completely confident that their care team has the data it needs, yet only 29 percent said all of their key providers can see the same data; 28 percent said only one provider can, and 25 percent said some do and some do not. Proactive use of the data is nearly absent: only 5 percent said their clinic uses CGM data to reach out between visits.

Research use is welcomed, with guardrails. Seventy-nine percent were very or completely comfortable with de-identified use of their data by providers and academic researchers. The conditions that build that comfort were, in order: true de-identification (72 percent), assurance the data would not be sold commercially (70 percent), a purpose limited to research or quality improvement (69 percent), seeing a summary of what was learned (65 percent), and the ability to opt out (59 percent). Independent ethics-board oversight ranked lowest, at 38 percent.

Insurer use of individual data is firmly rejected. Eighty-eight percent disagreed that insurers should use individual CGM data for approval or cost decisions, with 79 percent disagreeing strongly. Sixty-five percent

found insurer commercial use of even de-identified data unacceptable, and 69 percent said insurers should have no influence at all over which devices are covered.

Coverage protection was the single highest priority. When asked to rank what matters most, 60 percent placed "insurance coverage rules do not block CGM access" first, far ahead of safety and privacy (12 percent), proactive care-team use (10 percent), and unified provider access (8 percent). Counting appearances anywhere in the top three, coverage was named 92 times out of 100.

4.4 Survey 2: Data Use, Trust, and What Patients Want From Their Care Team

What we asked. Survey 2 was fielded from March to April 2026 and comprised 29 questions across five areas: respondent context and prior participation; how patients use and understand their own data and which care-team uses they value most; comfort with eight specific device-company data-use scenarios and the acceptability of specific insurer uses; lived experience of coverage, prior authorization, and required data sharing; and overall data-use stance with ranked trust priorities. Results were presented at Working Group Meeting 4. Three cross-cutting themes emerged from these findings, each with concrete policy implications.

Theme 1: "Use my data to help me, not control me"

Participants drew a sharp and consistent line between uses that serve them and uses that could be turned against them. Asked to characterize their overall stance, 59 percent said they are comfortable with research and product improvement uses but not with insurer or commercial uses, and a further 22 percent were comfortable with most uses of their de-identified data. Notably, no respondent rejected all use of their data beyond their own care.

Comfort with device-company use was high wherever the purpose was better devices and safer care: 87 percent were very or completely comfortable with use for improving sensor accuracy, 87 percent for developing automated insulin delivery algorithms, 85 percent for safety monitoring, 78 percent for academic research partnerships, and 74 percent for FDA regulatory submissions. Comfort softened for training artificial intelligence models within the CGM system (57 percent) and for demonstrating coverage value to insurers or employers (61 percent). The same logic governed which insurer uses patients would accept. As shown in **Table 3**, acceptance of care-supporting uses ranged from 37 to 67 percent, with only improved coverage reaching a majority, while acceptance of uses related to coverage eligibility or patient costs was much lower.

The underlying fear is concrete rather than abstract. Eighty-seven percent worried that glucose data could be used to deny or limit coverage, and 67 percent that it could raise their out-of-pocket costs. Asked what they would do if required to share CGM data to maintain coverage, only 15 percent said they would be comfortable; 39 percent would not want to share, 24 percent would share but feel uneasy, 17 percent said it depends on what data and how it is used, and 4 percent were not sure. When ranking what would most build their trust, the single most-cited first choice was an assurance that their data would never be shared with insurers for coverage decisions.

Table 3. Survey 2 respondents' acceptance of potential insurer uses of CGM data (n=46).

Insurer use	% who would accept
Care-supporting uses	
Improve coverage for diabetes services/devices	67
Provide data to academic researchers	46
Quality improvement / population health	43
Support care coordination, proactive outreach	39
Identify patients needing additional support	37
Control uses	
Eligibility or prior authorization decisions	11
Premiums or cost-sharing decisions	9

Policy implication: Patients draw a clear boundary: data may support care coordination, but not restrict coverage. This pattern held across both surveys, and it shapes the framing of **Recommendation 3** (Anti-Information Blocking) and the call in **Section 7** for clear policy boundaries on insurer use of device data.

Theme 2: Trust requires transparency, consent, and safeguards

Willingness to share is conditional. Participants identified several safeguards that would increase their comfort with device companies using their data. As shown in Table 4, transparency about how data would be used and the ability to opt out were selected most often.

Table 4. Factors that would increase Survey 2 respondents' comfort with device-company use of CGM data (n=46).

Guardrail	% selecting it as a factor that would increase comfort
Being told clearly what the data will be used for	76
Ability to opt out of specific uses	74
True, non-re-identifiable de-identification	65
Seeing a summary of what was learned	63
Explicit consent before use	61
Independent ethics-board review	48

What patients want first is to be told what their data will be used for and to be able to opt out of uses they do not want. De-identification and seeing a summary of what was learned followed closely. Explicit consent before use ranked somewhat lower, suggesting that respondents placed particular value on knowing what is happening with their data and retaining the ability to change or stop future use. Independent oversight was selected as a comfort factor by 38 percent of respondents in Survey 1, for provider and academic research use, and by 48 percent in Survey 2, for device-company use. When Survey 2 respondents were asked to name a single most important priority, independent oversight was chosen by 2 percent. The concerns behind that ranking are concrete: 61 percent worried about data being shared or sold without their knowledge, and 46 percent that they would not know what data an insurer holds or how it is being used. Respondents could select up to three concerns from the list.

Policy implication: For these respondents, patient control is the condition on which sharing rests. Opt-out rights, transparency disclosures, de-identification standards, and explicit consent before secondary use were the safeguards they named. Survey 1 points the same way: comfort with provider and academic research use of de-identified data was high, at 79 percent, where those safeguards were assumed. This finding shapes **Recommendation 1** (Patient Access Rights).

Theme 3: Patients want action and support, not just access

Access to CGM data is necessary but not sufficient. A gap between data availability and patient understanding runs across the surveys: only a third of respondents reported feeling well-informed about their CGM data.

- **52 percent** want help using CGM data to improve day-to-day management decisions
- **30 percent** want clearer explanations of what key metrics mean for their health
- **30 percent** want help understanding recommended glucose targets

Respondents want help using their data more than help understanding the terms. And they are a highly engaged group; if a third of them do not feel well-informed, the gap in the wider diabetes community is likely larger.

Asked what matters most when looking at their data, 87 percent named time in range and 74 percent named identifying actionable patterns; long-run trends (24 percent) and having data ready for appointments (22 percent) ranked lower. The same preference shaped what they want from their care team: 70 percent want personalized recommendations based on CGM trends, and 52 percent want proactive outreach when concerning patterns emerge, rather than waiting for the next scheduled visit.

Working Group discussion sharpened the picture. Participants described dissonance between what “good” looks like in a clinical encounter and what it looks like on a CGM display, leaving patients unsure which number to trust. Others questioned whether pushing time in range ever higher is always better, or can introduce its own burden. Advocates noted the gap is not only about patient understanding; it also reflects variation in clinician fluency with CGM data, differences in digital literacy, and inconsistency in how data is presented across receivers and apps. Several cautioned that closing the gap should not mean reintroducing burdensome manual logging that drives diabetes distress and technology fatigue.

Survey 1 pointed to the coordination dimension of the same gap. Fewer than a third of respondents were confident that all members of their care team see the same CGM data, and roughly a third reported acting as the go-between who relays data across clinics. Patients should not have to be their own integration layer.

Policy implication: Interoperability and data access must be paired with investment in interpretation support, including clinician-facing education, patient-facing tools, and proactive outreach workflows enabled by data flow. This finding shapes Recommendation 4 (Infrastructure Recommendations) and reinforces the supporting pathway of Adoption, Education, and Incentive Alignment across all six recommendations.

Theme 4: Coverage friction, and what patients have already lived

Survey 2 also asked what respondents had already experienced, rather than what they prefer.

In the twelve months before the survey, 43 percent of respondents went through prior authorization to start or continue using a CGM. Nine percent were asked to supply CGM data or documentation to justify continued coverage. Thirteen percent experienced a gap in access, and small numbers were forced to switch device brands or appealed a denial. Just over half, 52 percent, reported no coverage barrier of any kind.

Half of respondents (23 of 46) had gone through prior authorization or an appeal at some point and described the experience. Of those, 48 percent called it manageable but time-consuming, 26 percent stressful, and 22 percent straightforward. A further 43 percent had never gone through the process at all.

The concern that CGM data could be used against patients in coverage decisions is not hypothetical to this group: nearly one in ten has already been asked to hand over their data to keep their coverage. The trust findings in Themes 1 and 2 come from people with that experience.

4.5 Survey 3: From What to How

What we asked. Survey 3 was fielded from July to September 2026 and comprised 52 items. Its eight sections, in the questionnaire's own words, were: welcome and about you; making sense of your data; understanding what you agree to (terms and consent); directing your data and who receives it; insurer and third-party access; platform capabilities that build trust; consent that travels with you; and what matters most.

Surveys 1 and 2 established what patients want: responsible data use that helps them, trust built on transparency and consent, and support that turns access into action. They are less clear on the operational question that follows: by what mechanism. Patients want to know who can access or use their data and to be kept informed. What is not yet validated is the mechanism: the preferred form of notification and its cadence, the practical meaning of opt-out and revocable consent, the design of notification that helps rather than fatigues, and whether consent can travel with a patient across devices and clinics. Survey 3 is designed to test these operational approaches directly, so that the recommendations in **Section 6** can specify not only the mandate but a patient-validated path to meeting it.

What we found. Most respondents agreed to terms they had not fully read. Forty-two percent have never read a CGM device or app terms-of-use agreement in full, and another 39 percent have read one only partly; taken together, four in five did not read the terms in full before agreeing. Yet 63 percent rate their understanding of what they agreed to at 4 or 5 on a five-point scale. The remedy respondents select is not longer documents: 77 percent want a short up-front list of the key things they are agreeing to, 64 percent want plain-language summaries instead of long legal text, and just over half (53 percent) want the ability to see and change their choices later.

On how much control they currently have, respondents divide: 36 percent cannot say, one third want more, and 30 percent have about as much as they want. Expectations on withdrawal are pragmatic: 58 percent expect future sharing to stop while understanding that already-shared data may remain, while 21 percent expect deletion, an expectation current practice generally cannot meet. Asked what they would want when consent given to one provider or device is reused by another, respondents split almost evenly: 29 percent would approve any genuinely new purpose before it starts, and 27 percent would approve the arrangement once up front and be able to change it later. Both answers describe consent that can be revisited, not a signature given once.

When patients direct their own data, the acceptable circle of recipients is wide, and every member of it is chosen: their diabetes care team (89 percent), research collaborators (71 percent), other doctors or specialists they choose (70 percent), family members or caregivers they designate (62 percent), apps or tools they choose to use (51 percent), and a diabetes nonprofit or advocacy organization (27 percent). Only 13 percent would pre-approve none of these without case-by-case approval.

Toward payers, respondents want transparency first and narrow sharing. Sixty-five percent want notification every time a payer or third party accesses their CGM data and a further 24 percent would accept a periodic summary; 49 percent want notification the same day. On what they would share, 38 percent accept only pooled, de-identified data, 33 percent are not comfortable sharing any CGM data with an insurer or payer, and 20 percent accept a single derived summary number such as GMI, the current practice named in the question; individual-level review remains rare.

Preferences for staying informed do not converge. A periodic summary (40 percent) and alerts only when something new or unusual happens (38 percent) are effectively tied, and no option approaches a majority. For a new provider, respondents divide almost evenly among three options. The pattern argues for configurable notification rather than any single default.

Access itself is not the barrier: 84 percent almost always find the data they want on their own. What divides them is what to do next. Forty-five percent report no trouble adjusting their management from CGM data, while 26 percent understand the numbers but are unsure what to do about them; care-team time remains a tighter constraint than ability, 34 percent saying their care team consistently has time against 47 percent for ability. Asked for the single most important capability, respondents chose personalized recommendations based on their patterns (38 percent), far ahead of any alternative.

The extension added four caregiver respondents (4 percent), the first caregiver voices in this wave, and pediatric endocrinology settings (5 percent), largely though not entirely reflecting those caregivers.

Community and rural clinic representation remains minimal (2 percent), and the sample remains an engaged, predominantly adult-endocrinology CGM population, a limitation carried forward from Survey 2.

4.6 Voices from the Community

A small selection of participant comments, in their own words:

"Ensure data is used to improve care for all patients, not just for profit."

"My CGM data belongs to me. Using it without my knowledge or permission is theft."

"DO NOT SELL OR SHARE THE DATA. If I decide to give my data to you, I'm only giving it to YOU."

"As long as it's not used for coverage decisions, do whatever you like."

"CGM is a life-saving device; it should not be subject to the whims or cost-cutting measures of an insurance company."

"It's mine, not yours, period. Respect that and we're good."

"It should be freely available to me to use however I want, and not available to anybody else unless I fully give my consent."

"Trust depends on transparency, patient control, and making sure data is used to help people rather than judge them."

"Payers should know: if a patient has diabetes, CGM should be covered, data should not be required."

"Plain language is probably the biggest thing."

"I want my data to help me, not create more stress."

4.7 What We Heard Across All Three Surveys

Taken together, the surveys point to six priorities that shape this paper's recommendations:

- **Consent before secondary use:** Patients want explicit, informed consent and clear disclosure of secondary data uses before any sharing occurs.
- **Control they can exercise:** Patients want opt-out mechanisms that work and real agency over secondary use of their CGM data.
- **Support that turns access into understanding:** Patients want patient-facing tools and clinical support that close the gap between having data and knowing what it means.
- **Insurer uses patients reject:** Patients do not accept CGM data being used for coverage denial, premium setting, or prior authorization decisions.
- **Data flow that supports proactive care:** Patients want data to move well enough to support proactive outreach and personalized care between visits.
- **Oversight they can rely on:** Patients want CGM data use to be monitored and patient protections enforced.

These patients are not withholding their data. They support research, product improvement, and safety monitoring at very high rates, and not one respondent rejected all use of their de-identified data. What they ask is that the data be used to help them rather than control them, that they be told what is happening with it, that they be able to change their minds, and that access come with the support that makes it useful. The recommendations in **Section 6** respond to those asks.

5. Working Group Findings

This section summarizes the findings that emerged across the Working Group process. Positions are reported at the level of participant groups, without attribution to individuals or organizations. The findings reflect the authors' synthesis of what was heard rather than formally adopted positions of participating organizations; participation should not be interpreted as endorsement of every finding or recommendation. The findings are organized in four parts: areas where substantive alignment emerged across participant groups (5.1); areas where participants aligned on the goal but where mechanism and boundary questions remain open (5.2); the perspectives each participant group brought to the work (5.3); and the structural lessons the process confirmed (5.4). Where a finding shaped a specific recommendation, the connection is noted.

5.1 Areas of Alignment

Across the working group sessions, four areas of substantive alignment emerged among manufacturers, aggregators, participating clinicians, patient advocates, and quality organizations.

Patient Data Ownership and Direction

There is broad agreement that patients should have ultimate control over their device-generated data and that current proprietary systems create unacceptable barriers to patients directing their data to providers and trusted third parties of their choosing. This alignment is reflected in Recommendation 1 (Patient Access Rights).

FHIR-First API Direction

There is broad support for FHIR-based application programming interfaces as the technical foundation for CGM data exchange, with HL7v2 messaging acceptable where FHIR is not yet feasible. Multiple participants observed that these existing standards are appropriate, and that the primary challenge is modernization and adoption. This alignment is reflected in Recommendation 2 (Interoperability Standards).

The Need for Standardized Definitions

Participants agreed that inconsistent definitions of CGM metrics across manufacturers and aggregators create real downstream friction for clinical decision-making, quality measurement, and analytics. A structured review of implementations across five manufacturers and aggregators, documented in the CGM Data Dictionary (Appendix A), found broad consensus on what the core metrics are, with the variation concentrated in how they are computed and over what period. The most consequential divergence is in the observation window, which is anchored differently across platforms and is often configurable by the requesting clinician; because the same metric computed over different windows can yield different values for the same patient, this directly affects comparability. Time in Range and related metrics are further computed on a percentage-of-readings basis by some sources and a time-weighted basis by others, and minimum-data thresholds, wear-time methodology,[16] and unit and rounding conventions vary in ways that can affect values at clinically relevant thresholds and at thresholds that may be used in future quality

measures.[15] A shared CGM data dictionary that aligns where possible with USCDI, LOINC, and the iCoDE Core Dataset is broadly supported. This alignment is reflected in Recommendation 6 and the data dictionary in Appendix A.

Contracting Friction is a Real Barrier

Data aggregators and participating clinicians emphasized that lengthy, bespoke contracting processes create barriers to CGM data integration that are independent of, and often more limiting than, the technical barriers. Participants described negotiations stretching for months, and in some cases approaching a year, for what should be straightforward data exchange relationships. There is broad support among the participants who work inside these agreements for developing shared contracting principles that reduce friction while protecting intellectual property and patient rights. This alignment is reflected in Recommendation 5 and the principles in Appendix B.

5.2 Areas of Alignment with Open Questions

Participants also showed directional alignment in three additional areas. In each, there was broad agreement on the underlying goal, but less consensus on the appropriate mechanism, scope, or boundaries. These issues represent areas where the policy direction is clearer, even as important implementation questions remain unresolved.

Information Blocking Mechanism

There is consensus that current barriers to CGM data exchange are too high. There is less consensus on the mechanism for change. Three options are on the table: (a) voluntary industry alignment via shared principles and the CMS Interoperability Framework, (b) regulatory extension of the 21st Century Cures Act information-blocking framework to device manufacturers, and (c) TEFCA-tied participation that would extend information-blocking expectations through network participation. Each option has tradeoffs around speed, durability, and operational burden. This is the central open question for the policy framework; Recommendation 3 discusses the three options explicitly.

Intellectual Property and Liability

Device manufacturers raised legitimate concerns about protecting proprietary algorithms from reverse engineering through data granularity restrictions, and about liability exposure when device data flows through third-party systems and informs clinical decisions with potential adverse outcomes. The shared contracting principles in Appendix B propose specific framings for granularity and downstream sharing that attempt to balance these concerns with clinical and patient needs.

Insurer Use of CGM Data

Patient advocates and patients raised pointed concerns about whether patients should be informed if payers access their CGM data, about the emerging role of payers in device ecosystems, and about the possibility that insurers may use artificial intelligence to make compliance determinations affecting coverage decisions. The Survey 2 findings in **Section 4** sharpened this concern: 39 percent of respondents accept insurer use of CGM data for care coordination or proactive outreach, while only 11 percent accept

use for prior authorization and only 9 percent for premium decisions. Notably, this was an area of cross-group consensus rather than a patient concern alone; manufacturers likewise expressed strong reservations about insurer access to device data. The boundary is clear; the regulatory mechanism for enforcing it is not yet settled.

5.3 Participant Perspectives

Manufacturer and Aggregator Perspectives

Device manufacturers and data aggregators broadly support the API-forward direction signaled by HTI-5 and the CMS Interoperability Framework. They emphasized that adoption of existing standards is the harder problem than development of new ones and asked for clearer guidance on what good infrastructure looks like; aggregator participants in particular emphasized that practical, near-term progress depends on reducing contracting friction. Smaller manufacturers raised legitimate concerns about implementation capacity and the risk that requirements scaled to the largest companies would create competitive disadvantage. We address this in Recommendation 4 by proposing infrastructure expectations differentiated by capability where appropriate. We also flagged a concern raised across multiple sessions that policy framing should not focus only on CGM data platforms; EHR vendors are equally part of the system and their technical, financial, and contracting practices should be addressed as well.

Clinical and Implementation Perspectives

Clinical and implementation perspective was contributed by clinician-investigators on the project team practicing at large academic medical centers, reinforced by manufacturer and aggregator accounts of deployment experience. That experience is consistent: integration is rarely blocked by a single technical barrier. It is constrained by inconsistent interfaces, variable assurance practices, incomplete traceability, and operational fragility when systems move from pilot to durable, scalable implementation. These observations directly shaped Recommendation 4 and the shared contracting principles in Appendix B.

NCQA and Quality Organization Perspectives

The National Committee for Quality Assurance brought quality measurement perspectives to discussions of standardized metrics and data definitions. Quality measure development depends on consistent, comparable data; the core CGM metrics are well standardized, but variation in how they are calculated across platforms, even small variation, introduces heterogeneity that creates real barriers to using device data in quality programs and value-based contracts. NCQA's perspective extends beyond standardized and comparable metrics to the broader conditions needed for CGM-derived data to support quality measurement: data availability, structure, and interoperability are preconditions alongside standardized definitions. NCQA participation has been particularly important to Recommendation 6 and to the broader framing of CGM data as becoming core clinical infrastructure (**Section 2.4**).

Patient and Advocate Perspectives

Patient and advocate participation, beginning in November 2025 after a dedicated September 2025 orientation, has been central to the development of every recommendation. Patient priorities (**Section 4**)

shaped the framing of consent, transparency, opt-out, education, and insurer boundaries throughout this paper. Participating advocacy organizations contributed to working group discussions, and several also supported recruitment and dissemination for the patient surveys. Participation reflected real diversity of lived experience: people living with T1D, caregivers, and advocacy-organization representatives, several of whom are themselves people with T1D.

5.4 What the Working Group Confirmed

The cross-sector process confirmed three structural lessons that frame the recommendations in **Section 6**:

1. First, the policy gap for medical device data is real, widely acknowledged across participant groups, and not adequately closed by existing regulations.
2. Second, the technical foundations for closing the gap are largely in place; the work is to apply them.
3. Third, contracting and operational practices, not just regulation and technical standards, determine whether CGM data actually flows.

The policy recommendations that follow address all three.

6. Policy Recommendations

Drawing on the policy review, Working Group discussions, patient and caregiver survey findings, and supporting literature, we synthesized these inputs into six areas for policy action. The resulting framework moves from foundational rights to implementation and is grounded in existing statutory, regulatory, and standards-based authorities. Its core principle is that medical device data should align more closely with the frameworks governing electronic health information and interoperable health IT, particularly with respect to patient access, data sharing, interoperability, and information-blocking protections. The recommendations do not ask device manufacturers to become certified health IT. Rather, they call for a proportionate approach in which manufacturers make patients' CGM data available where patients and care teams need it, through a combination of voluntary alignment, standards adoption, guidance, and targeted regulatory action.

6.1 Implementation Pathways

Implementation can occur through different mechanisms, ranging from voluntary industry action to formal regulatory requirements. To clarify how the recommendations in this paper could be translated into practice, we organize the work along four primary pathways, complemented by two supporting pathways:

Primary pathway	What it does	Where it lives
1. Regulatory Change	Regulatory requirements and protections	Federal regulation, CMS policy, ONC authority
2. Certification & Standards	Technical interoperability expectations	FHIR, USCDI, certification requirements
3. Guidance & Clarification	Clarify expectations without mandates	HHS/ONC interpretation, federal guidance
4. Industry Consensus & Best Practices	Voluntary alignment to reduce friction	Contracting principles, shared conventions, cross-sector alignment

Supporting pathway	What it does
A. Implementation Tools & Shared Assets	Make implementation operationally feasible (data dictionaries, reference implementations, playbooks)
B. Adoption, Education & Incentive Alignment	Accelerate adoption and sustained implementation (patient and provider education, quality and reimbursement incentives, employer and payer expectations)

The four primary pathways represent increasing levels of policy force, from voluntary industry consensus and best practices, to federal guidance and clarification, to certification and standards requirements, to regulatory change. Different recommendations are best suited to different pathways depending on the nature of the problem, the authority required, and the degree of mandate needed. Each recommendation

below identifies the primary pathway proposed for implementation, along with supporting mechanisms where relevant.

6.2 Recommendation Summary

#	Recommendation	Existing authority	Primary Pathway
1	Clarify patient access rights for device data	HIPAA + HITECH §13405(e)	Guidance & Clarification
2	Extend interoperability standards to CGM data	21st Century Cures Act, HTI-1/HTI-4	Certification & Standards
3	Extend information-blocking protections to device platforms	21st Century Cures Act §4004	Regulatory Change
4	Define baseline infrastructure expectations	Modeled on ONC Health IT Certification Program	Certification & Standards
5	Develop shared contracting principles	TEFCA-like Common Principles approach	Industry Consensus & Best Practices
6	Develop and maintain a shared CGM data dictionary	USCDI / LOINC / iCoDE alignment	Industry Consensus & Best Practices

Each recommendation that follows is presented in a consistent structure:

- **Background and why it matters.** The problem the recommendation addresses and the stakes for patients, clinicians, and the system.
- **What patients and participants told us.** Survey findings and Working Group input specific to the recommendation.
- **Literature and policy precedent.** The evidence base and existing authorities the recommendation builds on.
- **The recommendation.** The specific policy action proposed.
- **Alternatives considered.** The principal options weighed against the recommended path.
- **Why we recommend this approach.** The reasoning for the path chosen.
- **Implementation pathways.** The primary and supporting mechanisms for putting the recommendation into practice.
- **Input we are seeking.** Open questions where consensus is not yet complete, posed to the groups whose input will settle them.
- **At-a-glance summary.** A closing table of what is proposed, its goal, policy alignment, and next steps.

6.3 Recommendation 1: Clarify patient access rights for device data

Existing authority: HIPAA + HITECH §13405(e)
Primary pathway: Guidance & Clarification
Clarify that medical device data is subject to existing patient access provisions, ensuring individuals can direct device data to any provider or trusted third party they choose.

Background and why it matters

Patient access to health information is the foundational right on which any modern health information policy rests. HIPAA established the right, and HITECH Section 13405(e) strengthened it by requiring electronic provision and the right to direct information to a third party of the patient's choosing. For CGM data, the key question is when those rights apply: HIPAA reaches device data maintained in a designated record set by a covered entity or by a business associate on its behalf, but it does not automatically reach data held independently by a manufacturer or device-data platform outside that relationship. Clarifying these boundaries, while promoting comparable patient-directed access across the broader device-data ecosystem, would support continuity of care, reduce friction in sharing CGM data, and reinforce patient agency over their health information.

What patients and participants told us

Survey 2 findings show overwhelming consensus among patients that their CGM data belongs to them and that they should determine who can access it. The 74 percent who consider opt-out rights important and the 76 percent who consider transparency important reflect a foundational expectation of agency. The pull quote from a participant captures the sentiment: *"My CGM data belongs to me. Using it without my knowledge or permission is theft."* Manufacturer and aggregator participants in working group sessions broadly affirmed this principle. The operating stance most industry and health-system participants articulated is that the patient owns the data and that organizations are stewards of it; several manufacturers state as much in their public privacy notices. The practical gap is that how laws and contracts actually assign control does not always track that stated principle. This recommendation is aimed precisely at that gap: aligning the rights and control patients have over device data with what already exists for other electronic health information under HIPAA, HITECH, and the Cures Act, so that the stewardship principle is made real in patients' ability to direct their data. Survey 3 answers these questions directly. When data is directed to a new provider or third party, no single form of notification commands a majority: respondents divide closely among a combination of a summary and a fuller record (28 percent), a periodic summary of access (25 percent), and an always-available record they can check at any time (24 percent), which argues for layered access, a summary first with the full record available, rather than a single artifact. On cadence, a periodic summary (40 percent) and alerts only for something new or unusual (38 percent) are effectively tied with no majority option, so sufficiency without burden is achieved by configurable notification with sensible defaults rather than a fixed schedule; delivery channel was not fielded. The entities patients would pre-approve as trusted third parties for patient-directed sharing are, in order, their diabetes care team (89 percent), research collaborators (71 percent), specialists they choose (70 percent), designated family (62 percent), apps they choose (51 percent), and advocacy organizations (27 percent); only 13 percent decline to pre-approve any category without case-by-case approval.

Relevant literature and policy precedent

HHS Office for Civil Rights has issued substantial guidance on the HIPAA right of access, including on an individual's right to direct protected health information to a third party under Section 13405(e).[34] The regulatory scope of that third-party direction was narrowed in 2020, when a federal court vacated its extension beyond electronic protected health information maintained in an electronic health record; the statutory right itself remains.[35] The 21st Century Cures Act information-blocking framework reinforces electronic access expectations for certified health IT. The CMS Interoperability Framework Criteria 1 through 5 explicitly extend patient access expectations to all data on the network. What is missing is clear federal guidance affirming that medical device data is subject to these same access rights when held by entities operating within the covered-entity perimeter or when patients seek to direct device data to third parties of their choosing.

Recommendation

HHS and ONC should publish guidance clarifying that medical device data, including CGM data, is subject to existing patient access rights under HIPAA and HITECH Section 13405(e). The guidance should affirm that patients can direct device data to providers and trusted patient-designated third parties of their choosing, including clinical teams, research collaborators, and patient-selected applications. Guidance should also identify the entities subject to these rights, including manufacturer cloud platforms operating as business associates and aggregators operating under business associate agreements. The guidance should also make clear that access is meaningful only when it can be exercised through a reasonable and proportionate process, rather than one whose complexity or delay defeats the right in practice.

Alternatives considered

We considered other approaches to strengthen patient access rights for device-generated data, including industry self-regulation:

Industry self-regulation and voluntary alignment. Manufacturers and data aggregators could voluntarily adopt common principles for patient access and data direction, and several companies have already taken steps in this direction through patient portals, APIs, and data-sharing capabilities. Voluntary action has the advantage of being relatively fast and adaptable and can allow technical solutions to evolve without waiting for federal action. Its principal limitation is inconsistency: access mechanisms, permitted uses, contractual restrictions, and technical capabilities vary across companies, leaving patients with different rights and experiences depending on which device or platform they use. Voluntary alignment alone therefore does not establish a reliable baseline across the market.

Why we recommend this approach

Federal regulatory guidance offers the strongest near-term path because it can clarify how existing patient-access and data-direction rights apply to medical device data without creating a new statutory framework. It builds on authorities that already exist, can provide greater consistency across manufacturers and aggregators than voluntary industry action alone, and can be implemented more readily than new rulemaking. Guidance can also address areas of current ambiguity, including how these rights apply to

manufacturer cloud platforms, aggregators, and patient-directed sharing with third parties. Voluntary industry alignment should continue in parallel.

Implementation pathway

Primary: Guidance & Clarification. HHS Office for Civil Rights guidance on right of access, complemented by ONC interpretive guidance on information blocking and device data.

Supporting: Adoption, Education & Incentive Alignment. Patient and clinician education campaigns; manufacturer playbooks for patient-directed exchange; quality program credit for patient-directed data flow where appropriate.

Recommendation 1 at a glance

Element	Summary
What it is	Clarify that medical device data, including CGM data, is subject to existing patient access rights under HIPAA and HITECH §13405(e).
Goal	Enable patients to direct their CGM/device data to any provider or trusted third party they choose.
Policy alignment	HIPAA Right of Access; HITECH §13405(e); 21st Century Cures Act access expectations; CMS Interoperability Framework Criteria 1–5.
Proposed implementation pathway	Primary pathway: Guidance & Clarification (HHS/OCR + ONC interpretation).

6.4 Recommendation 2: Extend interoperability standards to CGM data

Existing authority: 21st Century Cures Act, HTI-1/HTI-4
Primary pathway: Certification & Standards

Establish a FHIR-first pathway for device-data exchange and expand USCDI to include essential CGM data elements needed for safe, meaningful exchange.

Background and why it matters

Interoperability is foundational to every other recommendation in this paper. Without standardized, scalable APIs and a defined data model, patient access becomes bespoke, information blocking is difficult to enforce, infrastructure expectations vary by vendor, and contracts must repeatedly negotiate what should be settled technical questions. The cumulative effect of HTI-1 through HTI-5 has been to establish FHIR as the expected technical foundation for certified health IT exchange. CGM data should be in that foundation.

CGM also provides a practical proving ground for broader device-data interoperability. It is widely used, generates large volumes of clinically meaningful longitudinal data, and already has an established ecosystem of manufacturers, aggregators, EHR integrations, and implementation guidance. Establishing a durable approach for representing and exchanging CGM data can therefore inform how other forms of device-generated health data are incorporated into federal interoperability standards over time.

What patients and participants told us

Manufacturer and aggregator participants broadly agreed that FHIR-based APIs should be the technical foundation for CGM data exchange, with HL7v2 messaging acceptable where FHIR is not yet feasible. Multiple participants observed that adoption of existing standards is the harder problem than development of new ones. Health system representatives emphasized that scaling integration depends on consistent interfaces; one-off integrations per vendor are not sustainable. Patient survey data does not speak to API standards directly but is consistent with proactive, integrated care delivery (**Section 4, Theme 3**), which depends on technical interoperability.

Relevant literature and policy precedent

ONC certification requirements under HTI-1 through HTI-5 have progressively elevated FHIR APIs aligned to US Core. The CMS Interoperability Framework requires FHIR APIs conforming to US Core and USCDI v3 by July 4, 2026 (Criteria 13 through 15). The iCoDE project established technical standards and implementation guidance specifically for CGM-EHR integration.[11] USCDI does not yet include CGM-specific elements, though patient-generated health data is referenced in implementation guidance; USCDI v3 remains the certified baseline, and published versions now run to v7 (July 2026), none of which names CGM data elements. Working group participants noted that device-data inclusion is realistically a multi-cycle effort, making USCDI v8 or later the realistic target, and that complementary standards work is already underway (for example, the Caliper project and HL7 efforts on device data). A practical question raised in session is what it means for an exchange standard built around discrete data elements to accommodate CGM, which can generate hundreds of readings per day and potentially thousands of values

in a single inter-system exchange. The technical foundation is largely in place; what is missing is explicit inclusion of CGM data elements in the standardized data set and resolution of these volume and representation questions.

Recommendation

ONC should specify FHIR as the preferred API standard for CGM and other device-generated health data exchange, with HL7v2 messaging acceptable as a transitional standard, and should expand USCDI to include essential CGM data elements needed for safe, meaningful exchange. Essential elements should include, at minimum, measured and derived clinical values and metrics, device and sensor identifiers, and relevant contextual and event metadata. A more detailed set of core CGM data elements is provided in the CGM Data Dictionary in Appendix A. Transitional implementation expectations may be appropriate where technical maturity varies across manufacturers, but should be time-limited and designed to preserve a clear path toward FHIR-based exchange.

USCDI incorporation can proceed on two timescales. In the near term, CGM summary metrics can flow as laboratory values under existing USCDI classes, because established LOINC codes fit the laboratory data model; several health systems already ingest them this way. Over time, USCDI should establish a dedicated class for medical device generated data, which would recognize that device data are not laboratory tests and would make EHR support for device data a baseline infrastructure expectation rather than an optional add-on to be arranged with each vendor.

Alternatives considered

We considered two principal alternatives:

- **FHIR-only mandate.** Cleanest, but creates compliance risk for vendors not yet at full FHIR maturity, particularly insulin device manufacturers where infrastructure is less mature than CGM.
- **Vendor-defined approach.** Lowest implementation burden, but perpetuates fragmentation and bespoke integrations.

Why we recommend this approach

A FHIR-preferred pathway, with HL7v2 messaging acceptable as a transitional standard and coupled with USCDI expansion, recognizes the current state of vendor capability while setting a clear trajectory toward modern API standards, and it allows differentiated expectations by manufacturer size or capability where appropriate.

Implementation pathway

Primary: Certification & Standards. ONC Health IT Certification Program plus FHIR/USCDI implementation expectations.

Supporting: Implementation Tools & Shared Assets. Reference implementations, the CGM data dictionary (Appendix A), and iCoDE-aligned implementation guides.

Recommendation 2 at a glance

Element	Summary
What it is	Specify FHIR as the preferred API standard (HL7v2 messaging acceptable transitionally) and expand USCDI to include essential CGM data elements.
Goal	Scalable, standardized device-data exchange that reduces fragmentation and supports coordinated care.
Policy alignment	21st Century Cures Act; HTI-1 through HTI-5; CMS Framework Criteria 13–15 (FHIR/US Core, USCDI v3 by July 4, 2026); iCoDE.
Proposed implementation pathway	Primary pathway: Certification & Standards, working through existing bodies; CGM inclusion targeted at USCDI v8 or later (v3 remains the certified baseline).

6.5 Recommendation 3: Extend information-blocking protections to device platforms

Existing authority: 21st Century Cures Act §4004
Primary pathway: Regulatory Change

Clarify whether and how information-blocking protections should apply to medical device manufacturers and intermediaries, with safeguards that balance safety, intellectual property, and patient rights.

Background and why it matters

The 21st Century Cures Act prohibits practices that interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information by healthcare providers, certified health IT developers, and health information networks. Information blocking exceptions are limited and narrowly defined. CGM data held or exchanged by these covered actors (e.g., when integrated into the EHR) may therefore be subject to information-blocking protections. Manufacturer cloud platforms that hold the primary record of CGM data, however, often operate outside the health IT developer actor category because they do not develop or offer certified health IT, and they may not otherwise qualify as covered actors.

The practical consequence is that contractual terms, restrictive licensing language, integration costs, and proprietary design choices can functionally restrict legitimate CGM data exchange even when technical connections are available. Lengthy negotiations, bespoke agreements, and unclear permissions can slow integration for health systems, clinicians, and research collaborations. Although recent federal policy continues to refine information-blocking requirements for covered actors, the more fundamental question remains unresolved: whether and how comparable protections should apply to medical device manufacturers and device-data intermediaries that currently sit outside the framework.

What patients and participants told us

Patient survey responses captured how precarious access feels, and the fear that data access could be turned against patients. “Those improvements should be rewarded. My fear with insurance company access is that good control would instead be punished by limiting treatment,” one participant wrote. Working Group participants agreed that current barriers are too high. There was less consensus on the mechanism for change. Manufacturer participants raised legitimate concerns about safeguarding proprietary algorithms and managing liability. Aggregator and health system participants emphasized that contracting and operational practices, not just technical design, determine whether data actually flows. A concern raised across multiple sessions was that policy framing should not focus only on CGM manufacturers; EHR vendors and aggregators are equally part of the system. Reducing barriers to data flow and respecting the boundaries patients draw are complementary rather than competing: patients want CGM data to move without friction to themselves and their care teams, and firm limits and visibility where payers and third parties are concerned; only 11 percent consider payer access acceptable for prior authorization and 9 percent for premium decisions. Patients overwhelmingly want to know when a payer or third party touches their data: 65 percent want notification every time and a further 24 percent would accept a periodic summary, with 49 percent wanting same-day notice. What makes downstream flow feel

trustworthy rather than risky is scope: 38 percent accept payer access only to pooled, de-identified data, 20 percent accept a single derived summary such as GMI, which is current practice, and 33 percent are comfortable sharing nothing, while individual-level review is acceptable to almost no one. Transparency about access, paired with summary-level rather than stream-level scope, is the condition under which patients describe payer data flow as tolerable.

Relevant literature and policy precedent

The information-blocking framework at 45 CFR Part 171 is well-established for the actors it currently covers. The CMS Interoperability Framework Criteria 1 through 3 and Criteria 6 through 7 require that when patients or providers present valid digital credentials and purposes, all nodes return information they hold on the patient unless restricted by law. TEFCA participation creates network-level obligations that could in principle extend information-blocking expectations to participating entities, including device manufacturers and aggregators that choose to participate. Each pathway has been used in adjacent contexts but none has been applied specifically to medical device manufacturers.

Recommendation

Anti-information-blocking protections should be extended to medical device manufacturers and the intermediaries that operate device data platforms, through a phased approach. In the near term, federal agencies and industry should advance voluntary alignment through shared contracting principles (Recommendation 5), the CMS Interoperability Framework, and federal guidance establishing clear expectations against contractual, licensing, and operational practices that unnecessarily restrict legitimate device-data exchange. Over the longer term, ONC should consider extending relevant elements of the Cures Act information-blocking framework to medical device manufacturers and device-data intermediaries through rulemaking, with appropriate safeguards for intellectual property, patient safety, privacy, and legitimate technical limitations. TEFCA participation may complement either pathway by extending exchange obligations through voluntary network participation. More broadly, efforts to reduce information-blocking practices should address barriers across the full device-data ecosystem, including device manufacturers, aggregators, and EHR vendors, rather than focusing on CGM manufacturers alone.

Alternatives considered

We considered three pathways for extending information-blocking protections to medical device manufacturers and intermediaries:

Pathway	Strengths	Limitations
(a) Voluntary industry alignment	Fast to start; preserves flexibility; aligns with CMS Framework approach; minimizes regulatory burden	Variable adoption; no enforcement mechanism; may not survive personnel or strategy changes at individual companies
(b) Regulatory extension of Cures Act information-blocking framework to device manufacturers	Strongest legal anchor; consistent national baseline; existing enforcement infrastructure	Requires rulemaking with substantial industry process; ambiguity about which manufacturer activities are in scope; risk

Pathway	Strengths	Limitations
		of unintended consequences for legitimate IP protection
(c) TEFCA-tied participation extending obligations through network membership	Builds on existing federal infrastructure; ties obligations to benefits of network participation; flexible scope	TEFCA participation is voluntary; manufacturers may not have direct incentive to participate; partial coverage

We also considered whether CGM platforms should be brought within the ONC Health IT Certification Program itself. We did not recommend this approach. CGM cloud platforms have functions and design constraints that differ substantially from EHRs, and the existing certification framework may impose obligations poorly matched to device-data infrastructure. A more proportionate approach is to extend relevant information-blocking principles without requiring device platforms to become certified health IT.

Why we recommend this approach

No single pathway fully addresses the problem. Voluntary alignment offers the fastest opportunity to reduce friction and establish shared expectations, but it cannot ensure consistent adoption across the market. Regulatory extension offers the strongest and most durable national baseline, but requires greater policy development, stakeholder engagement, and safeguards against unintended consequences. TEFCA can reinforce either approach, but its voluntary nature makes it insufficient as the primary mechanism.

A phased approach therefore offers the best balance of near-term feasibility and long-term durability. It allows industry and federal agencies to begin reducing contractual and operational barriers now, while creating a pathway toward more formal protections if voluntary alignment proves insufficient. It also creates space to refine the scope of any future regulatory extension and develop appropriate safeguards for intellectual property, patient safety, privacy, and legitimate technical limitations before those requirements become mandatory.

Implementation pathway

Primary: Regulatory Change. 21st Century Cures Act information-blocking framework, applied through ONC rulemaking and ONC and Office of Inspector General enforcement mechanisms.

Supporting: Adoption, Education & Incentive Alignment. Federal guidance, CMS Interoperability Framework alignment, and quality program incentives that recognize alignment with anti-information-blocking principles.

Recommendation 3 at a glance

Element	Summary
What it is	Clarify whether and how information-blocking protections apply to device manufacturers and the intermediaries operating device-data platforms.
Goal	Reduce contractual and proprietary barriers to timely, complete, usable CGM data access for patients and providers.
Policy alignment	21st Century Cures Act §4004 (45 CFR Part 171); CMS Framework Criteria 1–3, 6–7; potential TEFCA-tied obligations.
Proposed implementation pathway	Primary pathway: Regulatory Change, proposed as a phased approach (voluntary alignment now, regulatory extension medium-term). EHR vendors, aggregators, and manufacturers all in scope.

6.6 Recommendation 4: Define baseline infrastructure expectations

Existing authority: Modeled on ONC Health IT Certification Program
Primary pathway: Certification & Standards

Define baseline infrastructure expectations for CGM and device data platforms that promote consistency, safety, interoperability, auditability, and patient-centered access.

Background and why it matters

APIs and exchange standards are necessary, but they are not sufficient to ensure that device data can be shared safely, reliably, and at scale. Recommendation 2 addresses how systems exchange data with one another. This recommendation addresses the capabilities that device-data platforms need within their own infrastructure to make that exchange possible, including secure access, authorization, auditability, data quality, operational reliability, and patient-directed sharing.

We do not recommend that CGM platforms be subject to the full ONC Health IT Certification Program. Device-data platforms and EHRs serve different functions and therefore require different technical and operational expectations. The certification framework is nevertheless a useful model: define a limited set of baseline capabilities that platforms should be able to demonstrate, while allowing flexibility in how those capabilities are implemented. Establishing those expectations would reduce variability across platforms, make integrations easier to assess and scale, and provide a more consistent foundation for the patient access, interoperability, and information-sharing goals described elsewhere in this paper.

What patients and participants told us

Participants agreed broadly that consistent infrastructure expectations would reduce the variability that currently makes integration painful. Health system representatives noted that they often have to recreate assurance through bespoke contracting, local governance, additional reviews, and technical controls when baseline expectations are unclear. Patient survey findings reinforced the need for capabilities such as audit logging (which makes consent and access transparent), event notifications (which enable the proactive outreach valued by 52 percent of respondents), and clear visualizations (which support the 70 percent who want personalized recommendations). Asked for the single capability that would most help them track and interpret their data, patients chose personalized recommendations based on their own patterns (38 percent), well ahead of attention-worthy-event notifications (19 percent), an access log showing who has viewed their data (13 percent), and simpler care-team sharing (11 percent); taken together, just over one in five (22 percent) selected a transparency capability, an access log or access control, as their top choice. On how clinically relevant notifications should be delivered, no cadence wins a majority; periodic summaries (40 percent) and unusual-event-only alerts (38 percent) are effectively tied, so helpfulness without alarm or fatigue points to user-configurable notification with conservative defaults rather than any fixed policy.

Relevant literature and policy precedent

In 2015, ONC finalized 60 certification criteria for health IT systems, organized into eight functional domains: Clinical, Care Coordination, Clinical Quality Measures, Privacy and Security, Patient Engagement,

Public Health, Design and Performance, and Transport Methods. Although subsequent rulemaking, including HTI-5, has proposed simplifying this framework, its underlying approach remains useful: identify the capabilities a system should demonstrate without prescribing exactly how they must be implemented. Device-data platforms do not require the full set of certification criteria developed for EHRs, but several domains are directly relevant, particularly care coordination and data transport, clinical functionality and quality measurement, privacy and security, patient access, and design and performance.

The CMS Interoperability Framework provides complementary precedent, including expectations related to purpose-of-use tagging, digital credentials, access control, audit logging, and security validation. Existing medical-device standards also offer important building blocks. The ISO/IEEE 11073 family addresses device interoperability, including ISO/IEEE 11073-20601 for personal health device communication,[36] while UL 2900-2-1 addresses software cybersecurity for network-connectable components of healthcare and wellness systems and is recognized by FDA for medical devices.[37] However, working group participants noted that some existing device standards were developed primarily for devices operating within institutional environments and do not fully reflect technologies such as CGM that generate and exchange data continuously across outpatient, home, and other care settings. This recommendation therefore builds on existing health IT and device standards while recognizing the need to adapt those principles to a more distributed device-data ecosystem.

Recommendation

Develop a defined set of minimum infrastructure expectations for CGM and device data platforms, organized around four functional domains: Care Coordination and Data Transport; Clinical and Clinical Quality Measures; Privacy, Security and Patient Rights; and Design and Performance. Twelve specific capabilities map to these domains:

#	Infrastructure capability
1	Standards-based CGM APIs (FHIR-first, SMART-capable)
2	Patient-directed access and app ecosystem for CGM data
3	Authorization and app registration with least-privilege access
4	Audit logging with patient-level traceability
5	End-to-end encryption and integrity controls
6	Standardized CGM data model, timestamps, and terminology
7	Bulk export/import for longitudinal CGM panels
8	Event notification and subscription for clinically relevant CGM events
9	Data provenance, data quality, and reconciliation
10	API observability, performance SLOs, and operational metrics
11	Clinician- and patient-friendly visualizations and displays

#	Infrastructure capability
12	Selective sharing, segmentation, and disconnection controls

These capabilities should align with existing standards (FHIR, USCDI, LOINC, iCoDE) and with the CMS Interoperability Framework where applicable. Expectations should be implemented in a phased manner consistent with manufacturer maturity, with clear sunsets for transitional accommodations.

Alternatives considered

We considered two principal alternatives to a defined set of minimum infrastructure expectations:

1. **Full certification of device-data platforms.** A formal certification regime would provide the strongest and most consistent assurance that platforms meet defined technical, security, and operational requirements. However, device-data platforms and EHRs serve fundamentally different functions, and applying the full ONC Health IT Certification Program to device platforms would introduce requirements that may not be relevant to their role. It could also create substantial implementation burden, particularly for smaller manufacturers, without necessarily improving the specific capabilities needed for safe and scalable device-data exchange.
2. **Voluntary industry best practices alone.** A fully voluntary approach would minimize regulatory burden and allow manufacturers to adapt implementation to their own platforms and technical maturity. It could also be implemented relatively quickly. Its limitation is consistency: without a shared baseline, health systems and other partners may continue to recreate assurance through local technical reviews, contracting requirements, governance processes, and security controls. That variability is itself a source of integration cost and delay.

Why we recommend this approach

A defined set of minimum infrastructure expectations offers a middle path between a full certification regime and purely voluntary best practices. It establishes a common baseline for the capabilities most important to safe, reliable, and patient-centered device-data exchange while avoiding requirements designed for fundamentally different health IT systems. Anchoring the framework to established certification principles and existing interoperability and security standards also allows the field to build on mature approaches rather than create a separate system from scratch.

A phased approach provides additional flexibility. Expectations can initially serve as a common reference for industry alignment and implementation, while over time selected capabilities could be incorporated into standards, certification-adjacent requirements, or quality and interoperability programs as the device-data ecosystem matures. This approach preserves flexibility in how individual platforms meet the expectations while creating greater consistency in what capabilities patients, clinicians, and health systems should be able to rely on.

Implementation pathway

Primary: Certification & Standards. Infrastructure expectations likely to emerge through ONC interoperability standards work and HTI-related requirements; CMS Interoperability Framework alignment provides a near-term voluntary pathway.

Supporting: Implementation Tools & Shared Assets. Reference implementations, shared infrastructure playbooks, and the data dictionary in Appendix A.

Recommendation 4 at a glance

Element	Summary
What it is	Define baseline infrastructure expectations for CGM/device-data platforms across four functional domains and twelve capabilities.
Goal	Consistency, safety, interoperability, auditability, and patient-centered access: the internal stack that makes Recommendations 1–3 possible.
Policy alignment	Modeled on ONC Health IT Certification framework; CMS Framework Criteria 22–26; standards including IEEE 11073 and UL 2900.
Proposed implementation pathway	Primary pathway: Certification & Standards, phased to manufacturer maturity. Distinct from Rec 2: this is intra-platform capability, not inter-system exchange.

6.7 Recommendation 5: Develop shared contracting principles

Existing authority: TEFCA-like Common Principles approach
Primary pathway: Industry Consensus & Best Practices

Develop shared contracting principles that reduce friction between manufacturers, aggregators, and providers, while respecting intellectual property and patient rights.

Background and why it matters

Technical interoperability alone does not ensure that CGM data can flow in practice. Manufacturers, aggregators, and health systems typically rely on contractual agreements to establish the terms under which device data can be accessed, integrated, and shared. When those agreements are lengthy, bespoke, or unclear about permitted uses and downstream sharing, they can become a barrier independent of the underlying technical capability.

Working Group participants described negotiations lasting months, and in some cases approaching a year, for data-exchange relationships that rely on otherwise established technical connections. These delays contribute to integration backlogs, increase implementation costs, and create variability in what patients and health systems are ultimately able to do with CGM data. Shared contracting principles could reduce that friction by establishing common expectations while preserving flexibility for organization-specific legal, commercial, and intellectual-property considerations.

What patients and participants told us

Participants described contracting as a major operational determinant of whether CGM data can be integrated into clinical and population-health tools. Provider organizations typically rely on agreements with data aggregators or directly with manufacturers to establish access to device data, and those arrangements were frequently described as lengthy and bespoke. Four recurring sources of friction emerged: EHR integration permissions, portability of consent across devices and platforms, restrictions on data granularity, and limitations on downstream sharing. These concerns were reported principally by data aggregator participants, whose role places them between manufacturers and health systems and therefore inside multiple contracting relationships across the ecosystem. They were also consistent with the clinical and implementation experience summarized in **Section 5**.

Patients did not discuss contracting directly, but they experience its consequences through whether their CGM data can move into the systems and tools that support their care. Their priorities, particularly that consent, transparency, and patient direction travel with the data establish important boundaries for any shared contracting principles. Appendix B reflects these themes. Patients describe portable consent as a standing, revisable authorization with purpose boundaries rather than a one-time signature: when consent given in one context is relied upon by another organization, the two leading expectations are effectively tied, approving any genuinely new purpose before it starts (29 percent) and approving the arrangement once up front with the ability to change it later (27 percent), and just over half of respondents (53 percent) want the ability to see and change their consent choices after the fact. What patients expect to see when an existing consent is relied upon favors living visibility over static records: an always-available record they can check (24 percent) and periodic summaries of access (25 percent) together far outweigh a one-time

record of what was agreed (8 percent). Contracting language for consent portability should therefore represent consent as purpose-scoped, patient-visible, and revisable, with withdrawal understood pragmatically; 58 percent expect future sharing to stop while already-shared data may remain.

Relevant literature and policy precedent

TEFCA's Common Agreement is the most relevant precedent: a national framework of common terms that reduce bilateral negotiation burden across participating networks. The Sequoia Project, CARIN Alliance, and CommonWell have developed similar shared frameworks at varying scales. The CMS Interoperability Framework adds complementary expectations around network transparency, performance, and standards-based connectivity that could inform common contracting principles. The iCoDE project has also begun developing shared conventions for CGM data exchange that may provide a more device-specific foundation for this work.

Recommendation

Develop shared contracting principles that address the four recurring friction patterns identified through participant engagement and illustrated in Appendix B: EHR integration permissions; portability of consent across devices and platforms; appropriate data granularity; and downstream sharing. The principles should establish common expectations that support patient-directed data exchange while preserving appropriate protections for privacy, security, and intellectual property. They should be developed through industry consensus, published as a public resource, and made available for voluntary adoption through bilateral relationships and alignment with broader interoperability initiatives such as TEFCA and the CMS Interoperability Framework.

Alternatives considered

We considered several approaches to reducing contracting friction reported by participants:

1. **Continued bilateral negotiation.** Individual negotiation between manufacturers, aggregators, and health systems preserves maximum flexibility and allows agreements to reflect the particular technical, legal, and commercial circumstances of each relationship. It is also the current state. However, participants described these negotiations as lengthy and highly variable, requiring organizations to repeatedly resolve many of the same questions about access, permitted uses, consent, data granularity, and downstream sharing. Continuing the current approach alone would therefore do little to address the friction this recommendation is intended to reduce.

2. **Standard industry contract templates.** Developing model agreements or standardized contract language could reduce negotiation even further by giving organizations a common starting point for device-data exchange agreements. Participants considered this potentially valuable, but also more ambitious than shared principles. Contract terms must accommodate differences in business relationships, legal requirements, technical architectures, and organizational risk tolerance, making a single template difficult to apply broadly. Developing and maintaining model agreements also requires substantial legal and industry engagement beyond the scope of this initiative. Standard contract templates remain a potentially valuable area for future work.

3. **Mandated contract terms through federal regulation.** Federal requirements could create the strongest and most uniform baseline and potentially eliminate some categories of restrictive terms altogether. However, prescribing detailed contractual language would substantially reduce flexibility, may exceed the appropriate scope of existing interoperability authorities, and could embed terms in regulation that need to evolve as technology and business models change. We therefore did not view mandated contract language as an appropriate near-term approach.

Why we recommend this approach

Shared contracting principles offer a practical middle ground between the variability of fully bespoke negotiation and the rigidity of standardized or mandated contract language. They can establish common expectations around the issues that repeatedly create friction while preserving flexibility for organizations to negotiate the specific legal, technical, and commercial terms appropriate to each relationship.

This approach is also feasible to begin through industry consensus without waiting for new regulatory authority. Published principles can serve as a common reference point for manufacturers, aggregators, and health systems, reduce the number of foundational issues that must be renegotiated in every agreement, and evolve as technology and implementation experience change. Over time, these principles could also provide a foundation for more formal model agreements or standardized contract language if the ecosystem determines that greater specificity would be useful.

Implementation pathway

Primary: Industry Consensus & Best Practices. Shared contracting principles informed by participant input, with illustrative framings in Appendix B, offered as a public resource for voluntary consideration. These are principles intended to reduce the time and cost of reaching agreements; they are not proposed contract language or a mandate.

Supporting: Implementation Tools & Shared Assets and Adoption, Education & Incentive Alignment. Illustrative framings in Appendix B; alignment with CMS Framework and TEFCA participation.

Recommendation 5 at a glance

Element	Summary
What it is	Develop shared contracting principles addressing recurring friction: EHR integration permissions, multi-device consent portability, data granularity, downstream sharing.
Goal	Reduce months-long bilateral negotiations while protecting intellectual property and patient rights.
Policy alignment	TEFCA Common Agreement model; CMS Framework Criteria 17–21; Sequoia/CARIN/ CommonWell precedents; iCoDE conventions as standardized technical exhibits that reduce what agreements must negotiate.
Proposed implementation pathway	Primary pathway: Industry Consensus & Best Practices; published as a public resource for voluntary adoption.

6.8 Recommendation 6: Develop and maintain a shared CGM data dictionary

Existing authority: USCDI / LOINC / iCoDE alignment
Primary pathway: Industry Consensus & Best Practices

Develop a shared CGM data dictionary with consistent definitions, calculation methods, and terminology standards, aligned with USCDI, LOINC, the AGP, and the iCoDE Core Dataset.

Background and why it matters

Standardized exchange is only useful if the data being exchanged have consistent meaning. Core CGM metrics such as Time in Range, Glucose Management Indicator, coefficient of variation, and percent active sensor time are generally similar across platforms, but differences in observation windows, calculation methods, data-sufficiency thresholds, and unit conventions can produce modest variation in reported values. For many patients, those differences may have little practical consequence. For patients near a clinical or quality-measure threshold, however, even small differences can affect interpretation, classification, or downstream action.

A shared data model therefore requires not only common transport standards, but also sufficiently consistent definitions and metadata to support reliable interpretation across systems. The goal is not to eliminate every implementation difference, but to standardize the parameters that materially affect comparability and ensure that relevant calculation context travels with the value. This is particularly important for clinical decision support, quality measurement, analytics, and research that depend on consistent interpretation across manufacturers and platforms.

What patients and participants told us

Manufacturer, aggregator, NCQA, and health system participants converged quickly on the need for standardized definitions and calculation methods. The dictionary review confirmed that the divergence across sources is largely one of implementation rather than intent: organizations broadly agree on what each metric represents, but differ in observation-window logic, calculation basis, data-sufficiency thresholds, and unit handling.

Two findings are especially relevant to policy. First, several contributors distinguish sensor-wear adherence from data sufficiency as separate constructs that a single metric is often asked to represent, suggesting that some metrics may benefit from companion measures rather than a single number. Second, at least one manufacturer already returns the applicable target range with every Time in Range value and transmits device metadata through its interface. Carrying this interpretive context alongside the metric offers a practical, low-friction path toward greater comparability.

All five contributors have indicated, without commitment, that they would be open to converging on a common methodology over time if doing so supported the adoption of additional CGM metrics into diabetes quality measures; together, these contributors represent a substantial share of the market. NCQA participation has been particularly important in this context because quality measurement depends on consistent, comparable data and may provide an important lever for adoption once standards are established. Quality-measurement participants also signaled that consistency in how wear time is

quantified would likely be a precondition for a metric such as Time in Range to be considered in future quality measurement. Patient survey participants did not address data definitions directly, but the finding that only a third feel well-informed about their CGM data suggests that the need for greater consistency and interpretability is not limited to the technical community.

Relevant literature and policy precedent

The iCoDE Core Dataset is the most directly relevant precedent.[11] USCDI defines the national core data set for interoperable exchange, but CGM-specific elements are not yet explicitly included. LOINC provides standardized terminology for many CGM metrics, while RxNorm and SNOMED CT serve related terminology functions for medications and clinical concepts. The CMS Interoperability Framework further reinforces the use of USCDI-aligned data and standardized terminologies. The CGM data dictionary in Appendix A builds on these existing standards by applying them to the specific definitions, calculations, and metadata needed for CGM data exchange.

Recommendation

Develop and maintain a shared CGM data dictionary with standardized definitions, calculation methods, and terminology, aligned with USCDI, LOINC, and the iCoDE Core Dataset, and consistent with the Ambulatory Glucose Profile specification where those metrics are surfaced in AGP reporting. Contributor confirmation should be sought for each metric, with alignment status (aligned / minor differences / under review) documented transparently. The dictionary should be maintained as a living resource, with a defined governance process for adding metrics, resolving definitional differences, aligning with USCDI revisions, and accounting for changes in widely adopted reporting specifications, including the AGP. The illustrative dictionary structure appears in Appendix A.

Alternatives considered

We considered two principal alternatives to a consensus-based data dictionary aligned with existing standards:

1. **Mandating definitions through certification requirements.** A certification-based approach could create the strongest and most uniform baseline. However, as discussed in Recommendation 4, a certification framework specifically applicable to device-data platforms does not currently exist, and creating one would be a substantially broader policy undertaking than is needed to establish common CGM definitions.

2. **Voluntary industry standards without alignment to existing frameworks.** Industry-developed definitions can be implemented relatively quickly and allow flexibility across manufacturers. However, without alignment to established standards such as USCDI, LOINC, and iCoDE, independent efforts could produce competing definitions or parallel terminology systems and perpetuate the fragmentation this recommendation is intended to reduce.

Why we recommend this approach

Industry consensus aligned with existing standards offers the most practical path to both consistency and adoption. The iCoDE experience demonstrated that standards developed collaboratively with the organizations that must implement them can achieve meaningful uptake while remaining technically feasible. The Ambulatory Glucose Profile is the strongest evidence available on this point: a voluntary consensus specification that achieved near-universal adoption across manufacturers and aggregators with no regulatory mandate behind it. Building on USCDI, LOINC, and iCoDE also avoids creating a new terminology framework and provides a clearer path for CGM data to integrate into broader interoperability and quality-measurement efforts.

The Working Group converged quickly on this approach, and the CGM data dictionary in Appendix A represents an initial implementation of that consensus. Over time, the dictionary can evolve as definitions mature, new metrics emerge, and CGM data become more fully incorporated into national interoperability standards.

Implementation pathway

Primary: Industry Consensus & Best Practices. Shared terminology standards anchored in the iCoDE framework and aligned with USCDI/LOINC; maintained as a shared resource under a defined governance process.

Supporting: Implementation Tools & Shared Assets and Adoption, Education & Incentive Alignment. Reference implementations; use of standardized definitions and calculation methods; manufacturer alignment as a CMS Framework participation criterion where applicable.

The dictionary review also clarifies how prescriptive standardization should be. Metrics that may be used in threshold-based quality determinations, with Time in Range a leading candidate, require standardization of the observation window, calculation basis, and data-sufficiency rule, because implementation variance at those points changes classification at the threshold. Descriptive metrics can tolerate more variation provided that the computing parameters travel with the value as metadata. The evidence therefore favors standardizing the parameters that affect comparability while requiring metadata disclosure elsewhere, rather than mandating a single implementation; this approach preserves room for manufacturer differentiation without sacrificing interpretability.

Recommendation 6 at a glance

Element	Summary
What it is	Develop and maintain a shared CGM data dictionary with standardized definitions, calculation methods, and terminology.
Goal	Comparable data across manufacturers for clinical decisions, quality measurement, analytics, and research.
Policy alignment	USCDI; LOINC; iCoDE Core Dataset; IDC AGP specification; CMS Framework Criteria 10, 13–14; NCQA quality-measure development.
Proposed implementation pathway	Primary pathway: Industry Consensus & Best Practices; maintained as a shared resource under a defined governance process; illustrative structure delivered as Appendix A.

7. Conclusions and Next Steps

The regulatory gap documented in this paper is specific and addressable. Existing health-information protections apply through defined regulatory relationships and actor categories, but they do not consistently reach the device manufacturers and platform operators that hold and route CGM data. In particular, many of these technology companies do not fall within the information-blocking framework's health IT developer category because they do not develop or offer certified health IT. Patients, clinicians, and health systems are therefore left to navigate fragmented access and exchange. Drawing on Working Group discussions, patient and caregiver surveys, policy analysis, and federal engagement, the Rising T1DE Alliance identified areas of cross-sector alignment and developed six recommendations for closing that gap.

The six recommendations are interdependent. Patient access rights depend on interoperability standards that make those rights actionable; interoperability depends on platform infrastructure and consistent data definitions; and scalable implementation depends on contracting approaches that allow data to move without repeated, bespoke negotiation. Progress in one area strengthens the others, while gaps in any one can limit the whole. CGM-EHR integration is already technically achievable and has been implemented at multiple institutions using iCoDE-aligned approaches and commercial integration platforms. What remains is to create the policy, standards, infrastructure, and payment conditions needed to move from isolated implementations to broad and durable adoption.

The current federal regulatory policy environment creates an important opportunity to do so. The CMS Interoperability Framework provides a voluntary blueprint across many of the domains relevant to CGM data exchange, while recent and anticipated ONC rulemaking continues to move certified health IT toward API-based interoperability and greater attention to device-generated data. The technical foundation is increasingly available. The next step is to apply these principles consistently to CGM data in ways that reflect what patients have told us: use the data to improve care, preserve patient direction and transparency, and pair access with the clinical action and support that make it meaningful.

A Foundation for Future Work

The Working Group process also identified several areas that require deeper work beyond the scope of the recommendations in this paper. Three priorities emerged in particular:

1. **Patient consent and data governance.** Additional work is needed to define how consent can be represented consistently across manufacturers, platforms, and APIs; how transparency and notification should follow data as they move across the ecosystem; and how patient preferences can be honored without creating unmanageable operational burden. More standardized and automated approaches to consent may also create new opportunities for responsible research and data sharing at scale.
2. **Device-data infrastructure.** Recommendation 4 establishes the need for baseline platform capabilities, but additional work is needed to determine which capabilities should constitute a

common minimum, how expectations should vary with technical maturity and organizational role, and which mechanisms are best suited to promote adoption. Manufacturer participants specifically identified this as an area where further cross-sector work would be valuable.

3. **CGM-based quality measurement.** Standardized definitions and calculation methods create the foundation for CGM-derived metrics to be used more consistently in quality measurement. This evolution has already begun: Glucose Management Indicator (GMI) is used in NCQA quality measurement through both the Diabetes Recognition Program and HEDIS, where it appears in the Glycemic Status Assessment for Patients With Diabetes measure. With a more standardized and interoperable data foundation, other CGM-derived metrics, including Time in Range, may become plausible candidates for future clinical quality measures. Measure development and specification appropriately remain the responsibility of quality organizations; the contribution of this work is to establish the consistent, comparable data foundation and cross-sector alignment that any future measure would require.

Each of these areas is substantial enough to warrant a dedicated workstream. This paper identifies them as priorities for future collaboration rather than attempting to resolve them within the current scope.

Next Steps

Policy progress requires specific commitments from specific groups. We offer the following next steps:

For regulators (CMS, ONC, HHS)

- Issue federal guidance clarifying that medical device data are subject to existing patient access rights under HIPAA and HITECH §13405(e) and that patients may direct those data to providers and other third parties they designate (Recommendation 1).
- Advance FHIR-based device-data exchange and expand USCDI to include essential CGM and other device-generated data elements through the established public standards-development process (Recommendation 2).
- Develop a pathway for extending relevant 21st Century Cures Act §4004 information-blocking protections to medical device manufacturers and device-data intermediaries, beginning with near-term guidance and voluntary alignment and progressing to rulemaking where appropriate (Recommendation 3).
- Engage industry, patients, and health systems in defining baseline infrastructure expectations for device-data platforms, using the CMS Interoperability Framework and future HTI rulemaking as potential pathways for adoption (Recommendation 4).

For CGM manufacturers and data aggregators

- Adopt FHIR-based APIs aligned to US Core so that patients' CGM data can reach the clinical systems where care decisions are made (Recommendation 2).
- Align with the shared contracting principles in Appendix B to reduce bilateral negotiation burden (Recommendation 5).

- Adopt the shared CGM data dictionary in Appendix A as a common reference, and contribute to the governance process Recommendation 6 calls for, under which it can be maintained over time.
- Implement the baseline infrastructure capabilities described in Recommendation 4 through a phased approach and participate in the CMS Interoperability Framework where appropriate.

For health systems and providers

- Adopt the contracting principles as a default starting point for device data agreements (Recommendation 5).
- Adopt standards-based CGM-EHR integration to improve documentation, reduce clinician and staff burden, and enable care-coordination, remote monitoring, and population-health workflows (Recommendations 2 and 4).
- Provide patients with clear education about how CGM data are interpreted, shared, and used in care, addressing the interpretation gaps identified in **Section 4**.

For quality organizations and payers

- Support data availability, structure, and interoperability alongside standardized, comparable CGM definitions, creating an important adoption lever for Recommendation 6.
- Incorporate patient preferences and appropriate safeguards when CGM data are used beyond direct clinical care, particularly for coverage and benefit-design decisions (**Section 4, Theme 1**).
- Align value-based care and remote patient monitoring incentives with proactive, clinically integrated use of CGM data (Recommendation 4).

For patient advocacy organizations

- Use the framework and recommendations in this paper to support dialogue with stakeholders.
- Continue bringing patient and caregiver perspectives directly into device-data policy development, using structured engagement approaches such as the model described in **Section 3**.
- Bring the patient-centered guardrails identified through this work, including transparency, meaningful consent, appropriate opt-out mechanisms, de-identification where appropriate, return of findings, and independent oversight, into device-data policy discussions.

Closing

CGM data policy is not a niche concern. It is an early example of a much broader challenge: how health information generated outside traditional healthcare settings should move into, and contribute to, the care people receive. The approaches developed for CGM will help establish precedents for wearables, remote monitoring technologies, and other forms of patient-generated health data. The Rising T1DE Alliance will continue this work through dissemination, federal policy engagement, and collaboration with patients, industry, healthcare organizations, quality organizations, and the broader diabetes community. The opportunity now is to move from isolated technical success to a durable ecosystem in which patients can expect their device data to be available, understandable, and useful wherever their care occurs.

References

1. Beck RW, Riddlesworth T, Ruedy K, et al. Effect of continuous glucose monitoring on glycemic control in adults with type 1 diabetes using insulin injections: The DIAMOND randomized clinical trial. JAMA. 2017;317(4):371-378.

2. Centers for Medicare & Medicaid Services. Decision Memo for Continuous Glucose Monitoring (CAG-00431N). 2017.

3. Espinoza J, Xu NY, Nguyen KT, Klonoff DC. The need for data standards and implementation policies to integrate CGM data into the electronic health record. J Diabetes Sci Technol. 2023;17(2):495-502.

4. Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 17935(e) (2009).

5. 21st Century Cures Act, Pub. L. No. 114-255, § 4004 (2016).

6. Office of the National Coordinator for Health Information Technology. United States Core Data for Interoperability (USCDI). Available at: https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi

7. Office of the National Coordinator for Health Information Technology. Trusted Exchange Framework and Common Agreement (TEFCA). Available at: https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca

8. Centers for Medicare & Medicaid Services, Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology. Request for Information; Health Technology Ecosystem. 90 Fed. Reg. 21034 (May 16, 2025). FR Doc. 2025-08701.

9. Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology. Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions To Unleash Prosperity (HTI-5 Proposed Rule). 90 Fed. Reg. 60970 (December 29, 2025). FR Doc. 2025-23896. Docket ID: HHS-ONC-2025-0005.

10. Centers for Medicare & Medicaid Services. CMS Interoperability Framework. July 2025. Available at: https://www.cms.gov/health-technology-ecosystem/interoperability-framework

11. Espinoza J, Klonoff D, Vidmar A, et al. 2022 iCoDE Report: CGM-EHR Integration Standards and Recommendations. Diabetes Technology Society. November 2022. Available at: https://www.diabetestechnology.org/icode/

12. Pahud DR, Harris LA, Lockee B, et al. A Data-Driven Pediatric Type 1 Diabetes Population Health Model Within Specialty Value-Based Care. Submitted to Diabetes, Obesity, and Cardiometabolic CARE. 2026.

13. HL7 International, Orders and Observations Work Group. Continuous Glucose Monitoring Implementation Guide, Version 1.0.0 (STU 1). Health Level Seven International; 2025. Available at: https://build.fhir.org/ig/HL7/cgm/

14. IEEE/UL. IEEE 2621 Series: Wireless Diabetes Device Security (2621.1, 2621.2, 2621.3). Institute of Electrical and Electronics Engineers and UL; 2022.

15. 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.

16. Straton E, Majidi S, Perkins AG, Barber J, Wang CH, Streisand R. 2037-LB: Considerations for Calculating and Reporting CGM Wear-Time in Research Settings. Diabetes. 2025;74(Suppl 1):2037-LB. doi:10.2337/db25-2037-LB

17. Bergenstal RM, Beck RW, Close KL, et al. Glucose Management Indicator (GMI): A New Term for Estimating A1C From Continuous Glucose Monitoring. Diabetes Care. 2018;41(11):2275-2280.

18. National Committee for Quality Assurance. Glycemic Status Assessment for Patients With Diabetes (GSD). In: HEDIS Measurement Year 2026, Volume 2: Technical Specifications for Health Plans. Washington, DC: NCQA; 2025. (LOINC 97506-0.)

19. Bergenstal RM, Ahmann AJ, Bailey T, et al. Recommendations for Standardizing Glucose Reporting and Analysis to Optimize Clinical Decision Making in Diabetes: The Ambulatory Glucose Profile (AGP). J Diabetes Sci Technol. 2013;7(2):562-578.

20. Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology. Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions To Unleash Prosperity. Proposed rule. Federal Register. December 29, 2025. FR Doc. 2025-23896.

21. U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology. Statement of Organization, Functions, and Delegations of Authority; Office of the National Coordinator for Health Information Technology (reversion of ASTP/ONC to ONC). 91 Fed. Reg. 16204 (April 1, 2026). FR Doc. 2026-06284.

22. U.S. Department of Health and Human Services, Centers for Medicare & Medicaid Services. Statement of Organization, Functions, and Delegations of Authority (establishment of the Office of Health Technology and Products). 91 Fed. Reg. 35479 (June 11, 2026) (effective June 9, 2026). FR Doc. 2026-11743.

23. U.S. Food and Drug Administration. Integrated Continuous Glucose Monitoring System. 21 CFR 862.1355. Classification established by De Novo request DEN170088 (Dexcom, Inc.), order issued March 27, 2018.

24. Centers for Medicare & Medicaid Services. Medicare and Medicaid Programs; CY 2026 Payment Policies Under the Physician Fee Schedule (Final Rule). Federal Register. November 2025. (New remote patient monitoring codes CPT 99445 and 99470, effective January 1, 2026.)

25. American Medical Association. Current Procedural Terminology (CPT) 2026. Chicago, IL: American Medical Association; 2025. (CGM interpretation codes 95249, 95250, and 95251, the last requiring a minimum of 72 hours of data; chronic care management codes 99490 and related.)

26. UnitedHealthcare. Remote Physiologic Monitoring (RPM). Medical Policy. Effective date January 1, 2026 (implementation subsequently postponed). Available at: https://www.uhcprovider.com

27. UnitedHealthcare. Medical Policy Update Bulletin: January 2026; Implementation Delay: Remote Physiologic Monitoring (RPM). Available at: https://www.uhcprovider.com

28. Centers for Medicare & Medicaid Services. Medicare and Medicaid Programs; CY 2027 Payment Policies Under the Physician Fee Schedule and Other Changes to Part B Payment and Coverage Policies. Proposed rule. Federal Register. July 16, 2026. FR Doc. 2026-14327. (Comment period through September 14, 2026.)

29. Office of the National Coordinator for Health Information Technology. United States Core Data for Interoperability, Version 7 (Standard Document). July 23, 2026. See also ONC Standards Bulletin 2026-2. Available at: https://isp.healthit.gov/united-states-core-data-interoperability-uscdi

30. Covington & Burling LLP, Digital Health practice. Analysis of the ASTP/ONC HTI-5 Proposed Rule and anticipated HTI-6 rulemaking. January 15, 2026. (Documenting ASTP/ONC signals that an HTI-6 proposed rule could address EHR data exchange with wearable devices.)

31. California Assembly Bill No. 133 (2021–2022 Reg. Sess.), Statutes of 2021, Chapter 143; implemented through the California Health and Human Services Agency Data Exchange Framework.

32. New York State Department of Health, Statewide Health Information Network for New York (SHIN-NY), 10 N.Y.C.R.R. Part 300.

33. Espinoza J, Klonoff D, Carini S, et al. 2025 iCoDE Report: EHR Integration Standards and Recommendations for Insulin Delivery Data. Diabetes Technology Society. https://diabetestechnology.org/icode2. Published December 30, 2025. Accessed September 19, 2026.

34. US Department of Health and Human Services, Office for Civil Rights. Individuals' Right under HIPAA to Access their Health Information, 45 CFR § 164.524. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. Accessed September 21, 2026.

35. Ciox Health, LLC v. Azar, 435 F. Supp. 3d 30 (D.D.C. 2020). See also US Department of Health and Human Services, Individuals' Right of Access to Health Records: Court Order. https://www.hhs.gov/hipaa/court-order-right-of-access/index.html. Accessed September 21, 2026.

36. ISO/IEEE 11073-20601:2022. Health informatics — Device interoperability — Part 20601: Personal health device communication — Application profile — Optimized exchange protocol. International Organization for Standardization; 2022.

37. UL 2900-2-1. Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems. UL Standards & Engagement.

Appendix A: CGM Data Dictionary

Purpose

The CGM Data Dictionary establishes a shared reference for how core continuous glucose monitoring concepts and metrics are represented and calculated across manufacturers and data aggregators. The 2022 iCoDE core dataset defines the core CGM concepts and data elements, while the Ambulatory Glucose Profile (AGP) provides the reference definitions and calculation conventions for standard CGM metrics where applicable. The dictionary documents each concept's definition, unit, terminology mapping, and, for each participating organization, its alignment status and relevant implementation variations. The goal is not to adjudicate a single correct implementation method, but to make differences visible so that clinicians, quality organizations, researchers, and downstream systems can understand what a reported value represents and how it was produced.

Structure

Concepts are organized into three categories: glycemic outcomes, device utilization, and device information. For each concept, the dictionary records the applicable reference definition, terminology mapping, and contributor-specific implementation. Each contributor entry includes an alignment status together with details on observation periods, calculation methods, data-sufficiency rules, data-quality handling, recency, and other implementation conventions.

Legend

- **Aligned:** the assessed concept is consistent with the applicable iCoDE concept and, where applicable, its standard metric definition and calculation convention are consistent with AGP. Aligned does not imply identical operational implementation; implementation methods that vary across contributors are keyed by row and described in the full workbook.
- **Minor Differences:** the applicable definition or calculation convention differs from the reference in a documented, bounded way. Alignment statuses therefore describe consistency with the applicable reference concept or convention, while the implementation keys describe operational choices that may cause the same underlying data to yield different results.

How this dictionary was developed

Seven manufacturers and aggregators were invited to review a standardized workbook based on the 2022 iCoDE concepts and data elements and, where applicable, AGP metric definitions and calculation conventions. Five organizations provided input reflected here: Abbott, Dexcom, Glooko, Medtronic, and Tidepool. Two additional invitees, Senseonics and DreaMED, are recorded as not assessed. Contributor submissions were supplemented, where useful, by publicly available technical documentation and implementation materials, and contributors were given opportunities to review the resulting entries. Because participation was voluntary and the level of available implementation detail varied, the depth of documentation differs by contributor. The dictionary is a point-in-time snapshot of an evolving landscape, published as a record of practice as of the date of publication. Stakeholder review also identified questions that were not systematically assessed across all contributors, including range-boundary handling, precision

and rounding, wear-time definitions, where individual concepts are available or transmitted, and what constitutes operational implementation of terminology standards such as LOINC; these are recorded as priorities for a future revision.

Summary Alignment Table

The condensed table below shows alignment status by contributor for the fourteen assessed concepts and data elements. Detailed definitions, calculation methods, implementation conventions, and contributor-specific notes are maintained in the full dictionary.

Dimension	Status	What this means
Clinical use	**Established**	These CGM concepts and metrics are established in clinical practice today.
Metric definitions and calculation conventions	**Generally Aligned**	Assessed concepts generally align with the applicable 2022 iCoDE Core or Expanded Dataset concepts, and standard CGM metric definitions and calculation conventions generally align with AGP where applicable. Documented bounded differences are shown below.
Implementation methods	**Vary**	Participating organizations differ in how some metrics are operationalized, including observation windows, calculation basis, data-sufficiency requirements, and other implementation parameters. Differences that may affect comparability or threshold-based determinations are keyed (a–e) in the right-hand column and described below.

Concept*	Abbott	Dexcom	Medtronic	Glooko	Tidepool	Implementation methods that vary *(see key below)*
Mean Glucose	Aligned	Aligned	Aligned	Aligned	Minor Differences	**a, b, c**
GMI	Aligned	Aligned	Aligned	Aligned	Minor Differences	**a, b, c**
Glycemic Variability (%CV)	Aligned	Aligned	Aligned	Aligned	Minor Differences	**a, b, c**
TAR-VH (>250 mg/dL)	Aligned	Aligned	Aligned	Aligned	Aligned	**a, b, c, d**
TAR-H (181-250 mg/dL)	Aligned	Aligned	Aligned	Aligned	Aligned	**a, b, c, d**
TIR (70-180 mg/dL)	Aligned	Aligned	Aligned	Aligned	Aligned	**a, b, c, d**
TBR-L (54-69 mg/dL)	Aligned	Aligned	Aligned	Aligned	Aligned	**a, b, c, d**
TBR-VL (<54 mg/dL)	Aligned	Aligned	Aligned	Aligned	Aligned	**a, b, c, d**
Number of Days CGM Worn	Aligned	Aligned	Aligned	Aligned	Aligned	**a, c**
% Time CGM Active	Aligned	Aligned	Aligned	Aligned	Aligned	**a, c**
Reporting Period Start Date	Aligned	Aligned	Aligned	Aligned	Aligned	**a**

Dimension	Status				What this means	
Reporting Period End Date	Aligned	Aligned	Aligned	Aligned	Aligned	a
Device Identification & Settings	Aligned	Aligned	Aligned	Aligned	Aligned	e
CGM Manufacturer & Model	Aligned	Aligned	Aligned	Aligned	Aligned	e

Key (a-e): implementation methods that vary across contributors

- **a) Observation-window anchoring.** Contributors vary in both the reporting windows they support and how default or selected windows are anchored; for example, to a requested date range, fixed calendar-day boundaries, the processing day, or the most recent data point. The same underlying data may therefore be summarized over different spans.
- **b) Calculation basis**. Implementations may be record-based or time/duration-weighted. This affects calculations such as mean glucose, glycemic variability, and range percentages, particularly when sampling intervals are irregular or data are missing.
- **c) Wear-time methodology and minimum-data thresholds.** "Number of Days CGM Worn" and "Percentage of Time CGM is Active" are standardized concepts, but the operational methods used to calculate wear are not fully standardized. Contributors may use calendar or qualifying days, rolling 24-hour approaches, active-time/day-equivalent calculations, expected-reading coverage, or other methods. Metric-specific data-sufficiency thresholds also vary.
- **d) Unit and rounding conventions.** Platforms report in mg/dL, mmol/L, or both, and convert and round differently at band boundaries; a value that rounds into range on one platform can round out of range on another.
- **e) Device metadata.** What device information is captured, and whether identifiers are passed downstream into EHR flowsheets, differs by contributor.

Senseonics and DreaMED were invited but are not assessed in this table. The GMI formula in current use is under active revision by its authors; values in this dictionary reflect the formulations in production as of the publication date.

Cross-Cutting Findings

Across the five contributors, the assessed concepts are broadly consistent with iCoDE, and standard CGM metric definitions and calculation conventions are generally consistent with AGP where applicable. The more substantial variation lies in how those concepts are operationalized, including observation windows, calculation basis, wear-time methods, data-sufficiency requirements, units, rounding, and the contexts in which data are made available. Six themes recur.

Observation window and start logic. Contributors vary in both the reporting periods they support and how those periods are anchored. Depending on the platform and use case, a reporting window may be defined by explicit start and end dates, a preset interval, the processing date, the most recent data point, or fixed calendar or day/night boundaries. Fourteen days is a common default or recommended period but is not universally required. These choices can cause the same underlying CGM data to produce different summary values because calculations may include different spans of data. For quality measurement and other cross-platform uses, the observation period and anchoring convention therefore need to be explicit and reproducible.

Calculation basis. Time-in-range metrics may be calculated using equally weighted readings or by weighting readings according to the duration they represent; these approaches can produce different results when sampling is irregular. Similar differences occur for summary statistics: use of a time-weighted rather than arithmetic mean can propagate into GMI and coefficient of variation.

Wear time and data sufficiency. Number of days CGM worn and percentage of time CGM active are standardized concepts, but the operational methods used to calculate wear are not fully standardized.[16] Approaches include qualifying-day counts, rolling 24-hour methods, continuous day-equivalents based on active time, and interval-based calculations. Contributors also distinguish, to varying degrees, between sensor-wear adherence and data sufficiency, which are related but separate constructs.

Minimum data thresholds. The amount of data required before a metric is reported differs across contributors and across metrics. Notably, contributors apply materially different minimum-data requirements for GMI,[17] a metric already incorporated into national quality measurement.[18]

Metadata carried with metrics. At least one manufacturer already returns the applicable target range with every time-in-range value, and returns device identification and settings through its API. This practice of transmitting the interpreting context alongside the metric, rather than the bare number, is a promising and already-demonstrated path toward comparability. This review did not systematically distinguish between information captured internally, displayed in a contributor platform, exposed through partner or developer APIs, and transmitted into the EHR; that distinction remains an area for future assessment.

Units and threshold boundaries. Glucose values are stored and reported in either milligrams per deciliter or millimoles per liter, and the rounded thresholds used in the two unit systems are not mathematically identical at the boundaries: the internationally standard 3.9 to 10.0 mmol/L converts to 70.27 to 180.18 mg/dL. A system storing in one unit and reporting in the other inherits this offset, which, together with differing rounding conventions, can affect classification precisely at the thresholds where quality measures make determinations.

Status and Confirmation

All five contributing organizations (Abbott, Dexcom, Medtronic, Tidepool, and Glooko) have contributed and confirmed their dictionary entries. Entries incorporate contributor feedback and, where applicable, publicly available technical documentation reviewed during the assessment. The complete workbook, including each organization's detailed entry and any remaining implementation questions, is available on the Rising T1DE Alliance website. The dictionary is published as a point-in-time reference current as of the publication date.

Availability: The full dictionary, including concept definitions, calculation methods, reference terminology mappings, and contributor-specific implementation notes, is available online from the Rising T1DE Alliance**:** **https://risingt1dealliance.org/cgm-data-policy**. Terminology **(LOINC)** codes are provided as reference mappings and should not be interpreted as evidence that every contributor stores or transmits those codes operationally.

Appendix B: Shared Contracting Principles

Purpose: Identify recurring contracting friction points and propose balanced principles to streamline data sharing agreements while preserving appropriate protections for intellectual property, privacy, security, and patient rights. These principles are offered to reduce the time and cost of reaching data-sharing agreements; they are illustrative and voluntary, and are not proposed contract language or a mandate.

Status: Four friction areas were identified through participant interviews and previewed at WG#4; the principles were reviewed with participants at WG#5.

B.1 EHR Integration Permissions

Current approaches observed in industry contracting:

- **Open:** "You may push therapy data to EHR" (no friction).
- **Prohibited:** "You may not share data to patient's EHR under any circumstances."
- **Case-by-case:** "Requires manufacturer pre-approval for each EHR integration."

Proposed principle: Contract terms should not unnecessarily restrict clinically appropriate EHR integration or patient-directed data exchange. Notification or reasonable coordination requirements may be appropriate, but outright prohibitions on legitimate data exchange should be avoided. Such restrictions may also raise information-blocking concerns when a party to the arrangement is a covered information-blocking actor or when the restriction affects the conduct of such an actor.

B.2 Multi-Device Data Chain (Consent Portability)

Challenge: When Device A integrates data from Device B (for example, automated insulin delivery systems pulling CGM data from multiple manufacturers), Device A cannot authorize sharing of Device B's data, creating impractical "back to source" requirements.

Proposed principle: Consent and authorization should be portable across the device-data chain where legally and technically appropriate. Depending on the context, that authority may be anchored to either:

- **The patient**, for patient-directed sharing of their device data; or
- **The clinical relationship**, where data sharing occurs under an applicable HIPAA-covered relationship or business associate agreement.

B.3 Data Granularity

Challenge: Some agreements require aggregation (for example, hourly insulin totals) that loses clinical utility. Clinicians cannot distinguish between bolus timing scenarios with different therapeutic implications when only hourly aggregates are available.

Proposed principle:

- User-entered or initiated data → provide with timestamp.
- Algorithmically generated data → provide at a resolution sufficient to preserve clinical meaning and support therapy decisions.

The principle that clinically meaningful data granularity requires therapy-relevant time resolution rather than coarse aggregation.

B.4 Downstream Sharing Restrictions

Current approaches observed:

- **Prohibited:** "You may not share data further."
- **Limited:** "Display or patient care only; no R&D use."
- **Open:** "Patient-initiated sharing permitted."

Proposed principle: Patient-directed sharing should be enabled, subject to applicable privacy, consent, and legal requirements. Contract terms should not unnecessarily prevent patients from directing their data to providers or other third parties they designate.

B.5 Summary

Area	Friction	Proposed Principle
EHR Integration	Blocking or pre-approval requirements	Notification may be acceptable; outright prohibitions should be avoided and may raise information-blocking concerns
Multi-Device Data	Consent doesn't flow through device chain	Patient or clinic-anchored consent should be portable
Data Granularity	Over-aggregation loses clinical value	Timescale must support therapy decisions
Downstream Sharing	Blanket prohibitions	Patient-directed sharing should be enabled

Appendix C: CMS Interoperability Framework Alignment

Purpose: Map each of the six policy recommendations in **Section 6** to the specific CMS Interoperability Framework criteria they implement or advance.

The CMS Interoperability Framework, released July 2025, provides a voluntary blueprint comprising 26 criteria across five domains. The recommendations in this paper are designed to operationalize the Framework for device-derived data; they do not alter the Framework but provide a concrete implementation pathway for one of CMS's high-priority early-adopter categories (diabetes and obesity prevention and management).

C.1 CMS Framework Domains

Domain	Criteria range	Focus
I. Patient Access & Empowerment	1–5	Patients get all their data, from anywhere, via apps they choose; audit logs; consent travels
II. Provider Access & Delegation	6–9	Treatment access for validated providers; delegation to vendors; quality and claims-based queries
III. Data Availability & Standards	10–16	USCDI v3; FHIR/US Core APIs by July 4, 2026; bulk data; subscriptions; record locator services
IV. Network Connectivity & Transparency	17–21	Public listing; provider directory; query metrics; inter-network connectivity
V. Identity, Security & Trust	22–26	Purpose-of-use; IAL2/AAL2 credentials; access control; audit logs; HITRUST-equivalent security

C.2 Recommendation-to-Criteria Mapping

Rec #	Recommendation	CMS Domains	Specific Criteria
1	Clarify patient access rights for device data	I; V	I.1–5; V.22, V.24
2	Extend interoperability standards to CGM data	III	III.10–16; especially 13–15
3	Extend information-blocking protections to device platforms	I; II; V	I.1–3; II.6–7; V.22
4	Define baseline infrastructure expectations	III; IV; V	III.10–16; IV.20–21; V.23–26
5	Develop shared contracting principles	IV	IV.17–21
6	Develop and maintain a shared CGM data dictionary	III; I; II	III.10, III.13–14; I.1; II.6

C.3 Detailed Alignment Rationale

Recommendation 1: Clarify patient access rights for device data

CMS requires that patients, via apps of their choice, can access all their electronic medical information anywhere it resides on the network, including structured and unstructured data, with audit logging and consent handling (Criteria 1 through 5). Our recommendation makes explicit that device data is part of that "electronic medical information," and that patients can direct CGM and device feeds to any endpoint, consistent with lawful purposes and access controls (Criteria 22 and 24).

Recommendation 2: Extend interoperability standards to CGM data

CMS requires chart notes and documents in USCDI v3 formats (Criterion 10), timely queries (11), appointment and encounter details with commitment to FHIR APIs (12), and by July 4, 2026, FHIR APIs conformant to US Core and USCDI v3 with terminology compliance, plus FHIR attachments and subscriptions (13 through 15). Our recommendation specifies CGM and device content for USCDI and FHIR, ensuring that CGM time series, calibration, alarms, and derived metrics flow through the same APIs and record locator services (16) as other clinical data.

Recommendation 3: Extend information-blocking protections to device platforms

CMS expects that when patients or providers present valid digital credentials and purposes (individual access or treatment), all nodes must return the information they hold on the patient except where restricted by law (Criteria 1 through 3, 6 through 7, 22). Our recommendation applies this principle explicitly to device vendors, closing a loophole where CGM and device data could be technically connected but practically withheld or throttled in ways that frustrate the framework's goals.

Recommendation 4: Define baseline infrastructure expectations

CMS criteria assume networks will support FHIR APIs, USCDI v3, record locator services, standards-based inter-network connectivity, network-wide search, and strong identity/security controls including HITRUST or equivalent (Criteria 10 through 16, 20 through 21, 23 through 26). Our recommendation packages these expectations into a defined set of infrastructure capabilities for device data platforms, ensuring that any platform handling CGM and device data can reliably meet the same technical and security bars as other health IT.

Recommendation 5: Develop shared contracting principles

CMS requires that data networks agree to be listed as CMS-Aligned Networks, publish membership and endpoints in the CMS National Provider Directory, report metrics on queries, support standards-based inter-network connectivity, and enable network-wide or targeted patient record search (Criteria 17 through 21). Our shared contracting principles recommendation translates these transparency and connectivity expectations into common expectations for device ecosystems, reducing bespoke negotiation and helping ensure that CGM and device networks can plug into CMS-Aligned Networks using consistent legal and governance principles.

Recommendation 6: Develop and maintain a shared CGM data dictionary

CMS requires that data exchanged under the framework be USCDI v3-compliant and use standardized terminologies (LOINC for labs, RxNorm for medications, SNOMED for conditions), and appear in both human-readable and machine-readable forms (Criteria 10, 13 through 14). Our CGM dictionary recommendation operationalizes this for device data by defining precisely how CGM measurements, events, and derived metrics are represented, coded, and calculated. This ensures that when patients or providers query device data (Criteria 1, 6), the returned information is consistent, computable, and clinically interpretable across networks and vendors.

Appendix D: CMS RFI Response

Note: This is an abridged summary of the Rising T1DE Alliance's public comments submission. The complete text is available on the Rising T1DE Alliance website: www.risingt1dealliance.org/cgm-data-policy.

Title: Rising T1DE Alliance Response to the CMS and ASTP/ONC Request for Information; Health Technology Ecosystem.

Submitted: June 16, 2025 · File Code: CMS-0042-NC · RIN: 0938-AV68 · 90 Fed. Reg. 21034 (May 16, 2025) · FR Doc. 2025-08701

Executive Summary

RTA urged CMS and ASTP/ONC to extend the patient access, interoperability, and certification requirements that currently apply to electronic health records and certified health IT so that they also reach medical device data platforms. The central position was that device data portals should sit within the same regulatory framework as certified health IT, including FHIR API requirements, patient access standards, and the interoperability provisions of the 21st Century Cures Act. The submission argued that this alignment is a precondition for data-driven care models and for the sustainability of value-based care programs in diabetes.

Recommendations by RFI Section

PC-2. Patient data access and integration

Patients can reach basic claims data through existing channels, but continuous glucose monitor readings, insulin pump data, and other device-generated information remain in proprietary platforms. RTA recommended extending Patient Access API requirements to manufacturer data platforms; establishing USCDI compliance for device data portals through new certification criteria analogous to the ONC Health IT Certification Program; confirming patient rights of access, control, and portability over device-generated data; and applying same-day electronic access expectations to device-generated electronic health information, consistent with the patient access provisions of the ONC Cures Act Final Rule.

TD-7. USCDI expansion for medical devices

Current USCDI standards do not adequately describe medical device data. RTA recommended expanding USCDI to include standardized device data classes, defining data elements for continuous glucose monitors, insulin pumps, and other therapeutic devices, and establishing device interoperability requirements comparable to EHR certification criteria.

VB-3 and VB-4. Essential health IT capabilities for value-based care

Value-based care organizations lack access to real-time device data for risk stratification, care coordination, and outcome measurement. RTA recommended treating medical device interoperability as an essential

health IT capability for alternative payment models, requiring device data integration for diabetes-focused value-based programs, and establishing device data as a core element of population health analytics.

VB-11. Interoperability challenges in value-based care

The absence of standardized device data limits glucose pattern tracking, adherence monitoring, and care coordination. RTA recommended FHIR-based or HL7-based device data APIs as a condition of value-based care participation, device data reporting requirements for quality measurement, and protocols for timely data sharing across care teams.

Supporting Policy Framework

The submission set out four supporting positions. On ownership, it noted that device data has legally ambiguous ownership status and argued that patients should hold rights of access, control, and portability, and that ownership claims should not be used to limit sharing that is consistent with treatment, payment, and health care operations. On consent, it proposed explicit patient consent for uses beyond direct care. On standards, it proposed a FHIR-first approach with HL7 as an acceptable alternative, terminology work with professional societies to add device concepts to standards such as LOINC, conformance to an expanded USCDI, and bulk export through REST APIs in common formats. On information blocking, it proposed extending the Cures Act prohibitions to device platforms that hold electronic health information as ONC defines it, together with no-cost patient access and public, standards-based APIs.

Phased Implementation

RTA proposed a three-phase sequence: policy development in the first year, covering USCDI expansion, draft regulatory text, and certification criteria; industry engagement in the second year, covering implementation standards, FHIR API guidance, and patient education resources; and enforcement in the third year, covering certification of device data platforms, patient access and anti-blocking enforcement, and ongoing monitoring.

Closing position: RTA argued that medical device data, including continuous glucose monitoring and insulin delivery data, falls within the definition of electronic health information under the ONC Cures Act Final Rule, and that platforms holding, transmitting, or displaying that information should therefore be subject to the same access, interoperability, and information-blocking requirements applied to certified health IT.

Submitted by Juan Espinoza, MD, on behalf of the Rising T1DE Alliance.

Appendix E: HTI-5 Public Comments

Note: This is an abridged summary of the Rising T1DE Alliance's public comments submission. The complete text is available on the Rising T1DE Alliance website: www.risingt1dealliance.org/cgm-data-policy.

Title: ASTP/ONC HTI-5 Proposed Rule Public Comments — Advancing Safe, Scalable API-Based Interoperability for Diabetes Care

Submitted: February 26, 2026 · Docket ID: HHS-ONC-2025-0005 · RIN: 0955-AA09 · FR Doc. 2025-23896

Executive Summary

Rising T1DE Alliance supports ONC's HTI-5 Proposed Rule and its forward-looking direction to strengthen API-based interoperability, which is essential for modern diabetes care. Diabetes device data (CGMs, insulin pumps, smart insulin pens, blood glucose meters) too often remain difficult to integrate into EHR workflows in ways that are reliable, timely, and clinically actionable. While we support reducing unnecessary burden, we are concerned that deregulatory changes that weaken baseline certification assurances could shift security and operational risk onto healthcare organizations as API-enabled exchange expands. We urge ONC to retain or clearly replace minimum baseline expectations for auditability, authentication/authorization, encryption, and API performance transparency to ensure interoperability scales safely and sustainably.

Four Specific Recommendations

1. Audit logs and traceability for API access (minimum baseline)

ONC should ensure there is a consistent baseline for audit logging and traceability for API-mediated access to electronic health information, including who accessed data, what data was accessed, when access occurred, which patient records were accessed, and which authorization scopes were used. Without standardized auditability, health systems must recreate assurance through bespoke contracting and local controls.

2. Authentication and authorization expectations for app ecosystems

ONC should retain or specify baseline expectations for API ecosystem authentication and authorization, including a consistent approach to app identification, user identity, and authorization scope management; clear expectations for how authorization is granted, reviewed, and revoked; and practical expectations that support safe and scalable third-party access without increasing information-blocking risk.

3. Encryption expectations

ONC should preserve or define minimum expectations for encryption that align with the realities of API-enabled exchange, including encryption in transit for API traffic as a baseline and clear minimum

expectations for protecting electronic health information as it moves across systems, intermediaries, and authorized applications.

4. API performance and availability transparency

If ONC is advancing a FHIR-first interoperability direction, it should also ensure that API-based access is operationally real by promoting transparency around performance, including basic uptime and availability reporting, reasonable disclosure around latency and rate limiting, and practical mechanisms for healthcare organizations and app developers to assess whether API performance supports real-world clinical and patient-facing use cases.

Why This Matters for Diabetes Device Data Integration

Integrating diabetes device data into the EHR is rarely blocked by a single technical barrier. It is constrained by inconsistent interfaces, variable assurance practices, incomplete traceability, and operational fragility when systems move from pilot deployments to durable, scalable implementation. These are precisely the areas where clear, consistent baseline expectations can reduce burden for healthcare organizations and developers alike. When interoperability and assurance are inconsistent, organizations may limit integration or keep workflows outside the EHR, undermining the very outcomes the Proposed Rule seeks to advance.

Closing position: RTA respectfully recommends that ONC retain baseline security and assurance capabilities within certification where possible, and where not feasible, publish a clear minimum assurance set that reduces variability, limits burden-shifting, and supports safe, scalable API-enabled interoperability.

Submitted by Juan Espinoza, MD, on behalf of the Rising T1DE Alliance.

Appendix F: Glossary of Terms and Abbreviations

The following terms and abbreviations are used throughout this white paper:

AGP (Ambulatory Glucose Profile). A standardized report format for CGM data, developed through expert consensus led by the International Diabetes Center and maintained by IDC. It defines a consistent set of glycemic metrics and a consistent visual presentation, and is used across CGM and aggregator platforms.

API (Application Programming Interface). A defined software interface through which one system can request and receive data from another programmatically; the technical mechanism underlying modern health data exchange.

CGM (Continuous Glucose Monitoring). The use of a wearable sensor that measures glucose continuously, generating the device data streams this paper addresses.

CMS (Centers for Medicare & Medicaid Services). The federal agency that administers Medicare and Medicaid; its programs, payment rules, and Interoperability Framework shape how CGM data is used and reimbursed in practice.

21st Century Cures Act. Federal law enacted in 2016 that, among other provisions, prohibited information blocking and required standardized, API-based patient access to electronic health information.

Data aggregator. A platform that collects device data from multiple manufacturers, normalizes it, and routes it to clinicians, health systems, and other authorized recipients.

EHI (Electronic Health Information). The electronic health information covered by the Cures Act information-blocking rules, encompassing the electronic protected health information in a designated record set.

EHR (Electronic Health Record). The certified software systems in which clinicians document care; the primary destination into which CGM data must flow to inform clinical decisions.

FDA (U.S. Food and Drug Administration). The federal agency that regulates medical devices, including CGM systems, for safety and effectiveness.

FHIR (Fast Healthcare Interoperability Resources). An HL7 standard for exchanging health care information through APIs; the technical foundation this paper recommends for CGM data exchange.

GMI (Glucose Management Indicator). A CGM-derived estimate of average glycemia analogous to laboratory HbA1c, calculated from mean sensor glucose.

HEDIS (Healthcare Effectiveness Data and Information Set). NCQA's standardized performance measure set, used by most United States health plans to assess quality of care.

HIPAA (Health Insurance Portability and Accountability Act). Federal law enacted in 1996 establishing the foundational privacy and security framework for protected health information, including patient rights to access their own records.

HITECH Act (Health Information Technology for Economic and Clinical Health Act). Federal law enacted in 2009 that accelerated EHR adoption and strengthened HIPAA enforcement and patient access provisions.

HL7 (Health Level Seven International). The standards development organization responsible for widely used health data exchange standards, including FHIR.

HTI rulemakings. The series of federal Health Data, Technology, and Interoperability rules (HTI-1 onward) through which certification criteria, information-blocking provisions, and interoperability standards are updated.

iCGM (integrated Continuous Glucose Monitor). An FDA device classification (21 CFR 862.1355) for CGM systems designed to reliably and securely transmit glucose data to other devices and systems.

iCoDE (Integration of Continuous Glucose Monitoring Data into the Electronic Health Record). A consensus standards initiative defining how CGM data should be integrated into EHRs; its Core Dataset anchors the CGM Data Dictionary in Appendix A.

Information blocking. Practices likely to interfere with the access, exchange, or use of electronic health information, prohibited under the 21st Century Cures Act for the actors it covers.

Interoperability. The ability of different information systems and devices to access, exchange, and cooperatively use data in a coordinated manner.

LOINC (Logical Observation Identifiers Names and Codes). A standard terminology for identifying laboratory and clinical observations, including CGM-derived measures.

NCQA (National Committee for Quality Assurance). An independent quality organization that accredits health plans and maintains the HEDIS measure set.

ONC (Office of the National Coordinator for Health Information Technology). The federal office responsible for health IT certification, interoperability standards, USCDI, TEFCA, and information-blocking regulations.

Physician Fee Schedule. The annual CMS rulemaking that sets Medicare Part B payment policy, including the remote patient monitoring and CGM interpretation codes discussed in **Section 2.4**.

Prior authorization. A payer requirement that a service, device, or supply be approved in advance as a condition of coverage.

RPM (Remote Patient Monitoring). The collection and clinical review of patient physiologic data, such as CGM data, outside of in-person visits; billed under Medicare as remote physiological monitoring.

TEFCA (Trusted Exchange Framework and Common Agreement). The federal framework establishing a nationwide network-of-networks for health information exchange under common legal and technical terms.

Time in Range (TIR). The percentage of time a person's glucose values fall within a target range, typically 70 to 180 mg/dL; a core CGM-derived clinical metric. Related bands are abbreviated in Appendix A as TAR (time above range) and TBR (time below range), each split into high and very high, or low and very low.

US Core. The FHIR implementation guide that defines how USCDI data classes are represented and exchanged in FHIR-based APIs in the United States.

USCDI (United States Core Data for Interoperability). The standardized set of health data classes and elements designated for nationwide interoperable exchange.

Value-based care. Payment arrangements that tie reimbursement to quality and outcomes rather than to the volume of services delivered.

RISING T1DE
ALLIANCE

www.risingt1dealliance.org • risingt1dealliance@luriechildrens.org