



DATA ACCESS **PRINCIPLES & BEST PRACTICES**

for Introducing Technology into a Health System

October 19, 2026

TABLE OF CONTENTS

Section I – Introduction	2
A. Summary.....	2
B. Definitions.....	3
C. Goals	3
Section II – Primary Use Case & Benefits	4
A. Primary Use Case	4
B. Benefits of Responsible Data Access.....	4
Section III – Limitations and Disclaimer of Legal Advice.....	5
Section IV – Principles and Best Practices	6
1. Principle: Transparency and Clear Expectations	6
2. Principle: Responsible Data Stewardship	6
3. Principle: De-Identification as a Foundation for Innovation	8
4. Principle: Use AI and Advanced Analytics Responsibly	9

Section I – Introduction

A. Summary

These voluntary Data Access Principles and Best Practices (the “Best Practices”) have been developed by AdvaMed member companies to promote **trust, transparency, responsible data stewardship, and effective collaboration** between Medtech Companies and Health System Partners. Strong privacy and data protection practices are essential to maintaining patient trust. Patient trust, in turn, is a foundational enabler of healthcare innovation, research, and the responsible use of data. The Best Practices primarily address arrangements in which a Health System Partner evaluates, introduces, implements, operates, optimizes, or receives support for a Medtech Company’s product and/or service in the United States. They reflect a commitment by Medtech Companies to use data in ways that:

- Comply with all applicable federal and state laws for all data types;
- Improve health outcomes, increase efficiency, and advance patient care and public health;
- Support collaboration with Health System Partners; and
- Enable innovation, including AI and advanced analytics.

These Best Practices apply to the following categories of data used in connection with medtech products and services:

- Protected Health Information (PHI) regulated under HIPAA, including pseudonymized or coded data;
- Consumer health and personal data regulated under applicable federal and state consumer protection and privacy laws, including Section 5 of the FTC Act and the FTC Health Breach Notification Rule;
- De-identified data, as defined under applicable law;
- Pseudonymized or coded data;
- Aggregated data; and
- Device, operational, technical, administrative, and other non-personal data.

They apply where a Medtech Company acts as a covered entity, business associate, controller, processor, or another role recognized under applicable law. The application of these Best Practices depends on the role performed, the data involved, the relevant purposes, and the applicable legal framework.

The use of personal health data, pseudonymized data, de-identified health data, and non-personal data by Medtech Companies and Health System Partners aids in the development of diagnostics, treatments and cures; improves health care interventions and outcomes; enables research and evidence generation; drives technology innovation; supports patient safety, public health, and healthcare system sustainability; and enhances the quality and efficiency of health care delivery, with patients as the ultimate beneficiaries. See [*AdvaMed U.S. Health Data Privacy Principles*](#).

B. Definitions

“Best Practices” refers to this document as a whole.

“Data” means patient, clinical, device, product-performance, operational, technical, administrative, or other information accessed, generated, used, or shared in connection with the evaluation, implementation, operation, support, monitoring, or improvement of a medtech product or service.

“Health System Partner” means a health care provider, health system, hospital, clinic, or other healthcare organization that evaluates, acquires, implements, uses, or obtains a Medtech Company’s product or service, and is the counterparty with or from whom data is accessed or shared.

“Medtech Company” means a company that develops, manufactures, distributes, provides, installs, supports, or services a medical technology product or related service that adopts these Best Practices. Although developed by AdvaMed’s member companies, the Best Practices are drafted for broader voluntary adoption.

“Parties” means the Medtech Company and the Health System Partner participating in a Data access, use, or sharing arrangement.

C. Goals

These Best Practices are intended to help Medtech Companies and Health System Partners establish clear, practical expectations for Data access, use, protection, and sharing throughout the lifecycle of a medtech product or service. Appropriate Data access can help the Parties evaluate and implement technology, integrate it into clinical and operational workflows, optimize its performance and utility, monitor safety and quality, meet legal and regulatory responsibilities, and improve the technology and related services.

Protecting patient privacy and ensuring responsible stewardship of health data are essential to maintaining patient trust in healthcare systems and health technologies. Patient trust is a foundational enabler of healthcare innovation, research, evidence generation and the responsible use of data to improve patient outcomes and public health.

These Best Practices are intended to support a trusted and effective data ecosystem within the medical technology sector by promoting responsible data use while enabling innovation. They aim to provide a common framework that supports responsible reciprocal sharing of Data and insights by helping Medtech Companies and Health System Partners align on expectations for how Data—identifiable, pseudonymous, and de-identified—is accessed, used, and safeguarded.

The Best Practices are designed to ensure that Medtech companies comply with all applicable federal and state laws, advance patient care and health outcomes, support scientific research and evidence generation, contribute to public health objectives, encourage the responsible development of new technologies (including AI and advanced analytics), and enable the continued generation of insights that benefit Health System Partners, patients, and the broader healthcare system. At the same time, they reinforce the importance of complying with applicable laws and maintaining strong privacy and governance practices.

By establishing clear, flexible, and practical expectations, these Best Practices seek to foster collaboration, reduce contracting and implementation delays, improve interoperability and troubleshooting, support more effective monitoring, and enable each Party to access and use Data in ways that drive research, better clinical outcomes and patient experiences, greater efficiency, product & service improvements, and innovation, with patients as the ultimate beneficiaries.

Section II – Primary Use Case & Benefits

A. Primary Use Case

INTRODUCING / IMPLEMENTING MEDTECH IN A HEALTH SYSTEM

These Best Practices primarily address the introduction and support of a medtech product or service in a Health System Partner. Successful implementation may require timely and appropriate access to patient, clinical, device, product-performance, operational, technical, administrative, or related Data to support planning, configuration, integration, testing, validation, training, operation, troubleshooting, performance optimization, safety and quality monitoring, regulatory responsibilities (such as the collection of Real World Evidence (“RWE”), contractual obligations, and improvement of the technology and related services.

B. Benefits of Responsible Data Access

Adopting a shared framework produces benefits at two levels. At the framework level, common expectations reduce friction in contracting, make diligence and negotiation more predictable, support interoperability, and de-risk the arrangement for the Health System Partner.

The categories of Data typically involved are:

- **Patient / clinical data** — diagnoses, orders, results, and outcomes relevant to the product’s function. This may include data from before, during, and after the clinical encounter where the medtech product/service is utilized;
- **Device / product-generated data** — telemetry, logs, settings, utilization, and performance signals from the technology itself;
- **Operational / workflow data** — throughput, staffing and scheduling context, and the integration points needed to fit the product into care delivery; and
- **Related data** — for example, claims, financial, or environmental data where relevant to performance, safety, or value measurement.

At the engagement level, the Data itself supports four functional needs. Access to these Data supports:

SUCCESSFUL IMPLEMENTATION	Clinical, operational, and device configuration data enable a smoother go-live, integration, and workflow fit, and site-specific validation and calibration, reducing failed or delayed deployments.
OPTIMIZATION OF PERFORMANCE AND UTILITY	Adjusting the medtech device/service to optimize its safety profile, effectiveness for individual patients, the patient experience, and the efficiency of health care delivery.
SAFETY AND QUALITY MONITORING	Real-world evidence data collection that may be required of MedTech Companies on Device performance. Adverse event and outcome data to support patient safety, earlier detection of issues, post-market surveillance, and shared risk reduction.
IMPROVEMENT OF THE TECHNOLOGY AND RELATED SERVICES	Aggregated, de-identified real-world data drive continuous improvement, with resulting innovations flowing back to Health System Partners and future patients.

Section III – Limitations and Disclaimer of Legal Advice

LIMITATIONS AND DISCLAIMER

These Data Access Principles and Best Practices do not create or convey any legal advice and do not create any attorney-client relationship between AdvaMed and any party. They are not a substitute for qualified legal counsel. Parties in the medtech ecosystem are encouraged to consider obtaining their own legal counsel.

These Data Access Principles and Best Practices should be read and interpreted to be consistent with the ***Antitrust Guidelines for AdvaMed Activities***. They are not intended to supersede or alter the requirements of the Guidelines.

These Best Practices are voluntary in nature and are not intended to be incorporated by reference into contracts or to create representations, warranties, or obligations beyond those expressly agreed between the parties.

Section IV – Principles and Best Practices

BEST PRACTICES: KEY PRINCIPLES

1. Transparency and Clear Expectations
2. Responsible Data Stewardship
3. De-Identification as a Foundation for Innovation
4. Use AI and Advanced Analytics Responsibly

1. Principle: Transparency and Clear Expectations

1.1 Clearly describe data practices in contracts, documentation, and publicly available privacy disclosures.

Medtech Companies should communicate their data practices to the relevant audience in a clear and accessible manner, including by posting a publicly available privacy notice to their website and a Notice of Privacy Practices for HIPAA covered entities. This includes ensuring that contracts, user documentation, and public disclosures accurately reflect how data is collected, used, and protected.

Agreements with Health System Partners should identify the types of data that the Parties will collect, use, and disclose, as well as the roles and responsibilities of the Parties with respect to the data they handle. Agreements should articulate the purposes for which identifiable data is used, including PHI and other Consumer Health Data.

Privacy disclosures should be given to patients by Health System Partners and clearly articulate the purposes for which data is collected, used, and disclosed, while providing patients with opportunities to consent or authorize disclosure where required. Example purposes include improving product or service performance to support patient outcomes, developing new products and services, conducting research, advancing public health, and developing or enhancing advanced technologies, including AI. Disclosures should also describe, as applicable, the privacy rights available to patients and how those rights may be exercised. These disclosures should be reviewed and updated periodically to confirm they remain up to date and accurate.

2. Principle: Responsible Data Stewardship

2.1 Comply with applicable federal, state, and international privacy and data protection requirements

AdvaMed members commit to adhering to all applicable federal and state laws and regulations governing data use. This includes compliance with HIPAA where applicable, as well as current and future state privacy, consumer protection, and data security laws, and emerging federal, state, and global privacy frameworks that may apply to health-related data. These frameworks may include laws governing the collection, use, disclosure, or storage of personal data, as well as advanced processing activities such as the development and use of artificial intelligence.

AdvaMed Members agree to adhere to the [AdvaMed U.S. Health Data Privacy Principles](#) and federal and state laws as applicable.

2.2 Implement policies, procedures, and safeguards that align with federal and state law and are appropriate to the sensitivity of the data

Data protection measures, including policies and procedures, should be implemented in accordance with applicable law and tailored to the type and sensitivity of the data involved. A risk-based approach ensures that stronger safeguards are applied where risks to individuals may be more significant.

For example, in addition to federal and state laws applicable to such data, identifiable data—particularly health information—may require enhanced access controls, encryption, and monitoring, while de-identified data may be subject to proportionate but still meaningful safeguards. Medtech Companies should also implement administrative measures, such as employee training, role-based access controls, and incident response protocols, to support consistent and secure data handling.

2.3 Limit use of identifiable data to permissible purposes

Identifiable data should only be used for purposes that are necessary, legitimate, and consistent with legal and contractual obligations, including HIPAA and any applicable Business Associate Agreements.

For example, under current federal and state law, the use of identifiable data may be permitted to deliver and support products and services, fulfill contractual obligations with Health System Partners, ensure patient safety, advance public health, and comply with regulatory or reporting requirements. Additional permitted uses may include limited operational functions, such as billing, customer support, and quality assurance, where appropriate.

2.4 Limit retention of identifiable data.

Agreements with Health System Partners may provide applicable retention periods for identifiable data during or after the term of the agreement, taking into account applicable state and federal laws, the purpose for which the data was collected, and the need to support ongoing operations. Additionally, Business Associates must comply with legal and contractual requirements with respect to the return or destruction of PHI at termination of the applicable Business Associate Agreement.

2.5 Support accountability through internal governance, training, and oversight

Governance structures that promote accountability for responsible data processing and use, including employee training and oversight mechanisms should be established. Medtech Companies recognize the importance of consistently applying data practices across their organizations.

2.6 Facilitate responsible international health data flows

Medtech Companies operate within a global healthcare ecosystem where patient care, research, public health activities, product safety monitoring, regulatory compliance, and innovation may require data to be accessed, shared, or processed across jurisdictions. Medtech Companies should support responsible international data flows in accordance with applicable laws and appropriate safeguards while maintaining privacy, security, and patient trust.

2.7 Apply the same standards when providing data to Health System Partners

Where a Medtech Company provides De-Identified or Pseudonymized Data to a Healthcare Partner:

- Agreements should specify re-identification restrictions — and, for Pseudonymized Data, permitted uses, security requirements, who holds the key and when re-linkage is allowed;
- Data shared should be accompanied by appropriate context on methodology, limitations, and intended use, so that it is interpreted and used correctly; and
- Agreements should state the assumed regulatory status of data (De-Identified Data is subject to fewer restrictions; pseudonymized or coded data is more regulated).
- Examples of what a Medtech Company may responsibly share include de-identified benchmarking against peer sites within the same Health System Partner's organization, or against de-identified, aggregated external reference populations, population-health and operational insights derived from the deployment, quality and safety dashboards, and real-world evidence the Healthcare Partner can use for its own quality improvement, accreditation, or research.

3. Principle: De-Identification as a Foundation for Innovation

3.1 De-identify personal data using recognized legal and industry standards, including HIPAA-compliant methods where applicable

Medtech companies should use established de-identification standards, where applicable, to reduce the likelihood that data can reasonably be linked to identified or identifiable individuals. Where applicable, this includes using HIPAA-compliant methodologies such as Safe Harbor or Expert Determination. De-identified Data should not be used in ways that are misleading, unfair or harmful. Use of De-identified Data should contribute to efforts to deliver higher quality care, better health outcomes, and/or public health while promoting efficiency of health care delivery.

3.2 Regularly assess de-identification practices

Medtech Companies that de-identify personal data should regularly assess the effectiveness of their de-identification processes. Assessments of re-identification risk should take into account the specific context, available safeguards, and the likelihood that individuals could reasonably be identified as technologies and risks evolve.

3.3 Implement safeguards designed to prevent re-identification

Appropriate controls should be in place to reduce the risk of re-identification. These may include contractual restrictions, technical measures, and internal policies governing data access and use.

3.4 Provide reasonable assurance of de-identification and data safeguards

Medtech Companies should provide Health System Partners with reasonable assurance regarding their de-identification practices and technical safeguards, including safeguards designed to prevent re-identification. Such assurance may take the form of summaries, certifications or attestations, taking into account confidentiality, security and intellectual property considerations.

3.5 Take appropriate steps to address any identified de-identification errors

Medtech Companies that de-identify data should implement processes that enable them to promptly investigate and remediate issues that arise during the de-identification process or are identified later.

3.6 Address coded data as a distinct category

Coded data is data from which direct identifiers have been removed or replaced with a code, where a key or other means of re-linking to individuals exists. Under many legal frameworks, coded data generally remain personal data, and contractual restrictions on re-identification operate as safeguards rather than as a change in legal classification. Because re-linkage may be possible, coded data is not necessarily de-identified data and may remain subject to applicable legal and regulatory requirements depending on the relevant legal framework and the circumstances of processing. At the same time, coded pseudonymization is a recognized privacy-enhancing measure that can significantly reduce privacy risks while enabling valuable research, innovation, patient safety activities, and product development. The effectiveness of pseudonymization may depend on factors such as the separation of identifying information, governance arrangements, technical and organizational safeguards, and who has access to any re-identification key. Where the parties use coded data, the agreement should specify who holds the key, the conditions under which re-linkage is permitted, and the security and data-use controls that apply—comparable to those accompanying a HIPAA limited data set under a data use agreement. Where applicable law imposes more stringent restrictions on the onward provision of coded data, those restrictions should govern.

3.7 Arrangements with Health System Partners should permit the responsible use of de-identified data for lawful purposes.

Subject to applicable federal and state law, agreements should permit Medtech Companies to use De-identified Data for lawful purposes in accordance with agreed terms. Such purposes may include the following illustrative examples:

- Delivery and enhancement of products and services;
- Product development and performance improvement;
- Research and development, including clinical and real-world evidence;
- Supporting patient safety, improved health outcomes, and public health;
- Analytics and operational insights;
- To promote the availability of services that can help patients;
- Education and training; and
- Development and validation of AI/ML tools.

4. Principle: Use AI and Advanced Analytics Responsibly

4.1 AdvaMed Members should adhere to the *AdvaMed Principles for Artificial Intelligence in Medical and Digital Health Technologies*.

Medtech Companies should comply with contractual requirements governing the use of artificial intelligence, as well as all applicable state and federal laws. Industry frameworks, such as the AdvaMed

Principles for Artificial Intelligence in Medical and Digital Health Technologies, may serve as supplemental guidance but do not replace contractual or legal obligations.

In adherence to the AdvaMed Principles for Artificial Intelligence in Medical and Digital Health Technologies, where Medtech Companies collect Data to build AI/ML models and deliver AI-enabled solutions, they should do so in a transparent manner, supported by any notice, consent, or authorization required under applicable law. Medtech Companies should also deploy AI/ML-enabled solutions responsibly and take reasonable steps to identify and mitigate unwanted bias in AI/ML-enabled medical technologies.

4.2 Use data to develop AI/ML in ways that promote patient benefit and healthcare value

AI and advanced analytics should be applied to enhance care quality, improve health outcomes, and unlock substantial patient benefits. These tools should be leveraged to support the development of new diagnostics, treatments, and cures; improve the effectiveness of healthcare interventions and patient outcomes; enable valuable research; drive technological innovation; and contribute to higher-quality, more efficient healthcare delivery.

4.3 Incorporate risk-based governance, including evaluation of performance, safety, and potential bias

Subject to applicable federal and state laws, AI systems should be developed and deployed with appropriate oversight to identify and mitigate risks, tailoring oversight to the intended use and potential impact of the technology. This typically includes evaluating model performance to assess accuracy and reliability across relevant populations, assessing safety to reduce the risk of unintended harm, and identifying and mitigating potential bias that could affect fairness or outcomes.

AI/ML technologies should be tested and monitored on a risk-based basis throughout the product lifecycle to support reliability. Ongoing evaluations should be designed to maintain trust and effectiveness over time. Governance practices may include structured review processes, ongoing monitoring, and periodic reassessment as data inputs, use cases, and real-world conditions evolve.

4.4 Align practices with applicable legal frameworks and recognized standards

AI governance requirements are legally binding in certain jurisdictions and continue to develop in others. Medtech Companies should consider whether they are subject to such requirements, and, where they are, identify their role and the applicable risk classification of the AI they provide. Because products in development today will remain on the market beyond forthcoming compliance deadlines, Medtech Companies should take those timelines into account during product development. Medtech Companies should monitor developments in applicable laws, regulations, and guidance related to privacy, data use, and AI governance, and update their internal practices as appropriate. Established frameworks addressing risk management, data governance, and ethical AI can serve as a common reference point that promotes consistency across the industry. Most of these frameworks are advisory in nature and supplement rather than replace applicable legal and contractual obligations. Medtech Companies should implement human oversight of AI-based decisions where required under applicable law, assigning that oversight to persons with appropriate competence, training, and authority.

AdvaMed

DIGITAL
Health Tech

www.advamed.org

