Congenius

Congenius Whitepaper

The EU GDPR & HIPAA | Regulatory requirements, operational impact, & strategic implications

November 2026

By Jörg Dogwiler



MedTech companies operate in one of the most sensitive global data environments. Modern medical devices generate, process, store, and transmit vast amounts of health-related information - often across borders and through complex digital ecosystems.

In this whitepaper, our Founder Jörg Dogwiler shares a comprehensive overview of The General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the US including key similarities and differences, regulatory implications for medical device manufacturers, and governance, technical, and operational compliance considerations.

If you're a MedTech organisation executive, compliance officer, regulatory affairs professional, cybersecurity team member, or product leader, read on…





The data landscape in MedTech has evolved, with medical devices advancing from standalone hardware systems to digitally integrated platforms. Today's products include:

- Connected implantables
- Remote monitoring systems
- AI-powered diagnostic software
- Cloud-enabled therapeutic platforms
- Wearable health technologies

These systems routinely process patient identifiers, biometric data, diagnostic results, behavioural data, and longitudinal treatment information.

Health data is classified as highly sensitive under both the EU and US regulatory frameworks - so as digital transformation accelerates, privacy compliance has become a strategic requirement alongside safety, quality, and cybersecurity.

What do the GDPR & HIPAA cover?



The General Data Protection Regulation (GDPR) applies to:

- Organisations established in the EU
- Non-EU organisations offering goods or services to individuals in the EU
- Entities monitoring behaviour of individuals within the EU

Health data falls under “special categories of personal data” and is subject to enhanced protections.



The Health Insurance Portability and Accountability Act (HIPAA) applies primarily to:

- Covered entities (healthcare providers, insurers, clearing houses)
- Business associates handling Protected Health Information (PHI)

Medical device manufacturers may be subject to HIPAA when they act as covered entities or business associates handling PHI on behalf of covered entities. Integration with a provider system or operation of a patient portal does not, by itself, establish HIPAA applicability.

Core GDPR principles

GDPR establishes seven foundational principles:

1. **Lawfulness, fairness, and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality**
7. **Accountability**

For MedTech companies, these principles directly affect product architecture, data flows, and lifecycle management.

Core HIPAA components

HIPAA consists of three major rules:

1. **The Privacy Rule |** Regulates permissible uses and disclosures of PHI
2. **The Security Rule |** Mandates administrative, physical, and technical safeguards
3. **The Breach Notification Rule |** Requires notification to affected individuals, the U.S. Department of Health & Human Services, and, in the case of large breaches, the media

On 16 November 2026, HHS announced a HIPAA Privacy Rule final rule, expanding electronic access and care-coordination provisions. It'll become effective 60 days after Federal Register publication, with compliance required 180 days after effectiveness.

Legal bases for processing health data under GDPR

GDPR health-data processing generally requires BOTH an Article 6 lawful basis and an Article 9(2) exception.

Relevant exceptions may include:

- Explicit patient consent
- Medical diagnosis and provision of care
- Public health interest
- Scientific research with safeguards

Manufacturers must clearly define their role (controller vs. processor) in each use case.

Technical safeguards under HIPAA

Key technical requirements include:

- Access controls
- Unique user identification
- Encryption (addressable implementation specification under the current rule)
- Audit controls
- Integrity controls
- Transmission security

Data subject rights under GDPR

GDPR grants individuals extensive rights, including:

- Right of access
- Right to rectification
- Right to object (where applicable)
- Right to erasure (“right to be forgotten”)
- Right to data portability
- Right to restriction of processing
- Rights related to automated decision-making

For connected devices, enabling portability and erasure can require significant system design considerations.

Business Associate Agreements (BAAs) under HIPAA

MedTech firms acting as Business Associates must execute BAAs defining:

- Permitted uses of PHI
- Security responsibilities
- Breach reporting procedures

Failure to maintain proper BAAs is a frequent compliance gap.

Cross-border transfers under GDPR

Transfers to third countries require a valid Chapter V mechanism, such as:

- Adequacy decisions
- Standard Contractual Clauses (SCCs)
- Binding Corporate Rules (BCRs)
- Limited Article 49 derogations in specific cases

Furthermore, cloud-hosted medical platforms frequently trigger international transfer obligations.



What are the penalties for violations?



GDPR administrative fines can reach:

€20 million or 4% of global annual turnover



HIPAA violations result in tiered penalties:

Inflation-adjusted, tiered civil monetary penalties and annual caps under 45 CFR 160.404.

Amounts vary by culpability and are updated periodically, with criminal penalties applicable in qualifying cases.

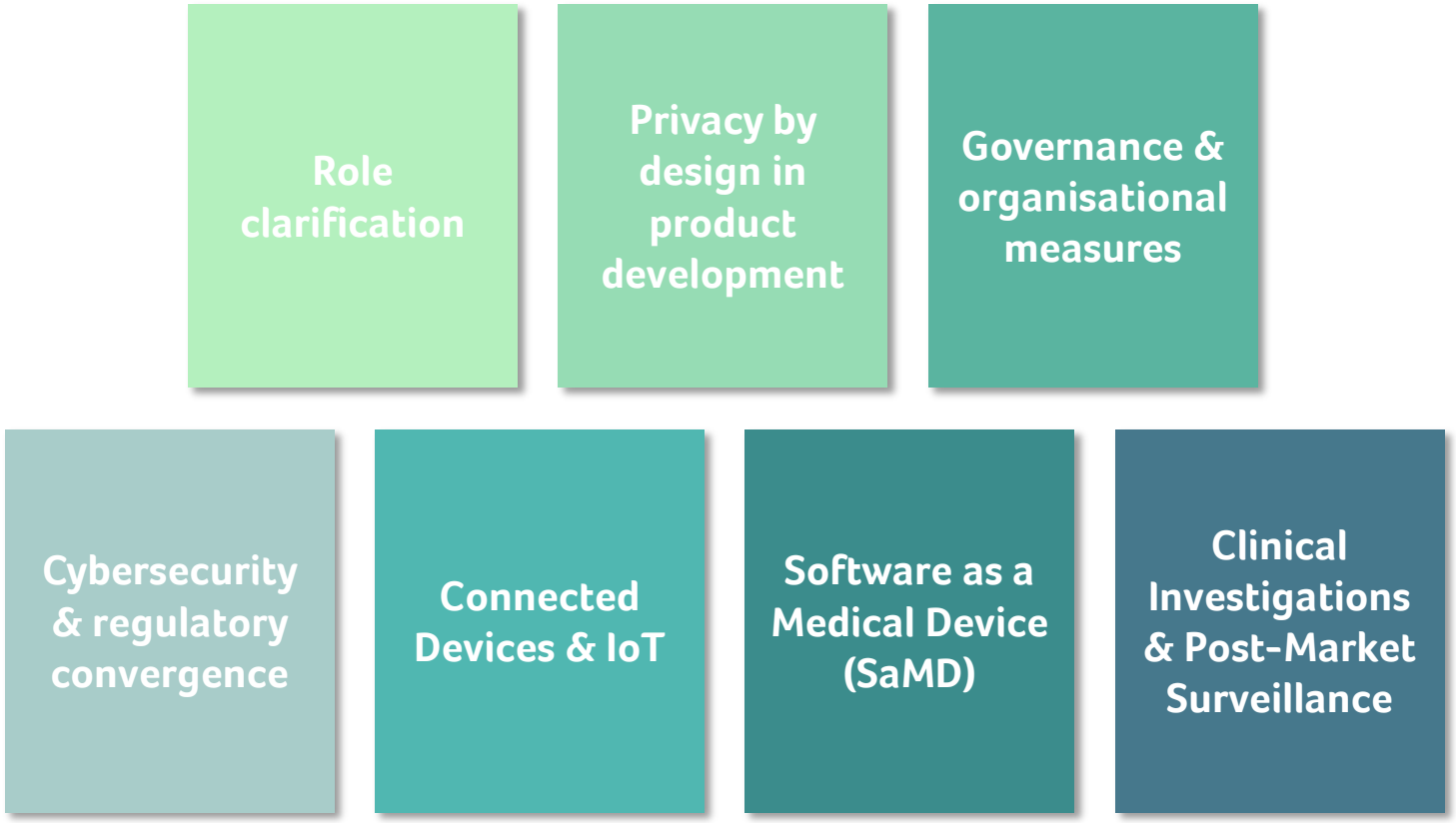
How do GDPR vs. HIPAA compare structurally?

GDPR establishes a comprehensive data protection regime across industries, whereas HIPAA focuses narrowly on healthcare-related PHI. As a result, multinational MedTech companies often adopt GDPR-level governance as a baseline global standard.

Dimension	GDPR	HIPAA
Regulatory scope	All personal data	PHI within healthcare ecosystem
Territorial reach	Global applicability	Primarily US-based
Legal basis required	Yes	Permitted use structure
Individual rights	Extensive	Limited
Revenue-based fines	Yes	No
De-identification standard	Pseudonymised data generally remains personal data; anonymised data sits outside GDPR only where individuals are no longer identifiable	Safe Harbour / Expert Determination method

What are the implications for medical device manufacturers?

Effective compliance with GDPR and HIPAA means that medical device manufacturers must pay special consideration to:



What are the implications for medical device manufacturers?

Role clarification

Who is the Controller vs. the Processor?

A recurring challenge in MedTech ecosystems is determining:

- Is the manufacturer a **controller**?
- A **joint controller** with the hospital?
- Or merely a **processor**?

Role clarity affects liability, documentation requirements, and contractual obligations – so it's important to **define roles at an early stage.**

Privacy by design in product development

Both GDPR and HIPAA emphasise proactive safeguards, with essential elements spanning the following:

- Data minimisation at architectural level
- Secure default settings
- Pseudonymisation where possible
- Logging and monitoring capabilities
- Encryption at rest and in transit
- Secure software development lifecycle (SSDLC)

Privacy must **be embedded into quality management systems** (QMS) alongside safety and performance.

What are the implications for medical device manufacturers?

Governance & organisational measures

Effective compliance requires structured governance:

- Data protection officer or privacy lead
- Internal privacy policies
- Vendor due diligence procedures
- Incident response frameworks
- Regular training programs
- Internal audit mechanisms

Documentation is critical for regulatory defensibility.

Swiss manufacturers should separately assess the Swiss Federal Act on Data Protection (FADP), in addition to GDPR/HIPAA where applicable.

Cybersecurity & regulatory convergence

Data privacy and cybersecurity are increasingly interconnected, with regulatory bodies worldwide now integrating cybersecurity requirements into medical device approval processes. Core measures include:

- Threat modelling
- Penetration testing
- Vulnerability management
- Patch governance
- Zero-trust architecture
- Continuous monitoring

For a robust approach, consider MDR/IVDR cybersecurity, privacy impact assessments, and AI governance together, while maintaining their distinct legal obligations.

What are the implications for medical device manufacturers?

Connected Devices & IoT

Key privacy challenges include:

- Continuous remote monitoring
- Cloud synchronisation
- Third-party integrations
- Mobile applications

Manufacturers must ensure:

- End-to-end encryption
- Secure authentication mechanisms
- Role-based access controls
- Secure firmware update processes

Software as a Medical Device (SaMD)

For AI-driven or cloud-based solutions:

- Secondary data use requires legal basis review
- Automated decision-making may trigger additional GDPR obligations
- EU AI Act obligations may also apply to qualifying medical-device AI; implementation dates and any amendments must be checked
- Data versioning and traceability are critical

Remember: Algorithm retraining must align with purpose limitation requirements.

What are the implications for medical device manufacturers?

Clinical Investigations & Post-Market Surveillance

Manufacturers routinely process personal data for:

- Clinical trials
- Vigilance reporting
- Real-world evidence
- Performance monitoring

To reduce compliance risk, we recommend clear separation between clinical, commercial, and R&D datasets.

How will data privacy maturity benefit your business?

Data privacy maturity has the power to support regulatory readiness, improve hospital procurement confidence, and facilitate cross-border expansion.

It also reduces litigation exposure, whilst boosting corporate reputation and investor confidence.

With healthcare providers increasingly assessing vendor privacy position during procurement, strong privacy governance is becoming a competitive differentiator.



A roadmap for implementation

Phase 1 | Data inventory & mapping

- ❑ Identify all data flows
- ❑ Classify personal data and PHI

Phase 3 | Control implementation

- ❑ Technical safeguards
- ❑ Organisational policies
- ❑ Vendor management processes



Phase 2 | Risk assessment

- ❑ GDPR: Data Protection Impact Assessment (DPIA)
- ❑ HIPAA: Risk analysis

Phase 4 | Monitoring & continuous improvement

- ❑ Regular audits
- ❑ Incident simulation exercises
- ❑ Regulatory monitoring

In conclusion...

The GDPR and HIPAA represent two of the most influential privacy frameworks worldwide.

While structurally different, both demand strong governance, robust technical safeguards, transparent processing practices, and accountability at executive level.

MedTech organisations that strategically integrate privacy into their core will be better positioned to navigate regulatory scrutiny, cybersecurity threats, and global market expansion - aiding their successful operation at the intersection of innovation, patient safety, and highly sensitive data processing.



Do you have a data privacy challenge related to a medical device? Our team is ready and happy to help – simply get in touch to start the conversation.

Contact us:

E: info@congenius.ch

T: +41 44 741 04 04

Congenius AG

Riedstrasse 1

CH-8953 Dietikon

© 2026 Copyright Congenius AG. All Rights Reserved.