

Wearable Medical Devices – What Should Your Contracts Look Like?

10-06-25 • alert • [katherine leibowitz](#)

Editor's Note: This article was selected as a featured editorial by Med Device Online on December 1, 2025. You can read the published version [here](#).

The wearable medical device industry sits at the intersection of life sciences regulation and rapidly-evolving technology law. Companies in this space face overlapping legal frameworks that can quickly become a minefield. Compliance obligations require careful navigation to avoid regulatory scrutiny, contractual inconsistencies, or costly product delays.

This blog post focuses on the contractual frameworks wearable companies must have in place to navigate that landscape. While the Food and Drug Administration (FDA) requirements shape device safety and marketing, day-to-day risk often turns on how companies handle HIPAA obligations, state privacy laws, artificial intelligence (AI) concerns, and the growing reality of multi-agency enforcement. These issues converge in the contracts that govern how wearable companies operate and protect their business.

In particular, we cover:

- Business associate (BA) responsibilities under the Health Insurance Portability and Accountability Act (HIPAA)
- Business associate agreements (BAAs)
- Services agreements with healthcare providers (HCPs)
- Essential website and portal terms
- Regulatory and enforcement risks across agencies

Imagine your company manufactures and sells a wearable medical device used in a doctor's office or prescribed for patients to use at home. We also assume that your wearable is already cleared or approved by FDA. The device collects patient readings, transmits them to your secure cloud system, and processes the results for physicians to view through a password-protected portal. If you handle protected health information (PHI) on behalf of covered entities (CEs), you are almost certainly a HIPAA business associate. For purposes of this post, we assume you are operating in that role.

Where Does Your Company Fit In?

In the U.S., wearable companies generally fall into three main regulatory categories:

1. If a company acts as a business associate and handles personal health records, it is subject to HIPAA's Privacy, Security, and Breach Notification rules and Section 5 of the FTC Act.
2. If a company does not act as a business associate but handles personal health records, it is subject to Section 5 of the FTC Act and the FTC's Health Breach Notification Rule.
3. If a company does not act as a business associate and does not handle personal health records, it is subject to Section 5 of the FTC Act.

Key Regulations:

- **HIPAA:** sets standards for protecting the privacy, security and permitted use and disclosure of PHI, and requires notification of breaches involving unsecured PHI.
- **Section 5 of the FTC Act:** Prohibits “unfair” or “deceptive” acts and practices, including misleading claims about how consumer health information is collected, used, or disclosed.
- **FTC Health Breach Notification Rule:** Requires certain organizations not covered by HIPAA (e.g. vendors of personal health records) to safeguard health data and notify consumers and the FTC about breaches involving unsecured identifiable health information. July 2024 amendments clarified its application to health apps, connected devices, and similar products.
- For further information on these regulations, refer to the FTC’s [resources](#) for compliance guidance.

We previously wrote [here](#) about consumer health data privacy initiatives by the FTC and the U.S. Department of Health and Human Services (HHS) that impact digital health technologies.

I. Business Associates

If your company creates, receives, maintains or transmits PHI on behalf of a CE, you are a BA and must comply with HIPAA. This often surprises wearable tech companies that hail from software startup backgrounds.

HIPAA for BAs

As a BA, you are subject to HIPAA’s extensive privacy and security obligations. For example, you must:

- Conduct a HIPAA risk assessment
- Implement administrative, physical, and technical safeguards, including robust policies and procedures for handling PHI
- Execute BAAs with CEs and other BAs as needed
- Limit use and disclosure of PHI to what is permitted under HIPAA and the BAA
- Report breaches of PHI to the CE

Avoid Common Pitfalls

HIPAA imposes significant obligations on wearable device companies that act as business associates. Many startups delay HIPAA planning until after obtaining FDA clearance or approval for their device. We have seen companies that needed to redesign aspects of their devices after FDA clearance or approval, sometimes requiring additional FDA review, because the companies started their regulatory process with clinical trials (where HIPAA obligations are met through HIPAA authorizations or IRB waivers), later to encounter HIPAA business associate compliance requirements.

Best practice: Build HIPAA by design into your product and operations to avoid costly redesigns or regulatory setbacks.

II. Key Written Agreements for Business Associates

A. Business Associate Agreement

As a BA, you will need to enter into a BAA with each HIPAA covered entity (such as physicians, hospitals, or clinics) whose PHI you handle. You will also need downstream BAAs with any subcontractors—such as your cloud service provider—who will have access to PHI. Having upstream and downstream BAAs maintains a compliant chain of trust.

- **BAAs must include:**
 - Permitted and required PHI uses and disclosures
 - Limits on PHI use and disclosure
 - Safeguarding requirements
 - Subcontractor compliance
 - Breach and security incident reporting
 - Assistance with CE HIPAA duties (e.g. access, amendment, accounting of disclosures of PHI)
 - Audit access by HHS
- **Optional provisions:**
 - Use and disclosure of PHI for the BA's own proper management and administration or to carry out its legal responsibility
 - The ability to de-identify PHI
 - Provision of data aggregation services
 - Obligations of the CE to the BA—including notifying the BA of limits on the CE's rights to use and disclose PHI that impact the BA downstream

Negotiation Tip: Because HIPAA mandates certain terms, many business associates assume BAAs are purely standardized documents. BAAs aren't one-size-fits-all. CE templates often favor the CE, with important nuances for BAs overlooked. For example, the BAA may contain detailed—and sometimes unrealistic—breach notification timelines and obligations. The BAA may also include unrelated business terms (liability caps, indemnities, insurance) that conflict with your underlying services agreement. Consider having your own BA-favorable template BAA.

B. Services Agreement with HCPs

As a BA, you will need a well-crafted services agreement with the HCP to complement your BAA. The services agreement is essential for defining expectations, protecting your business, and ensuring operational clarity.

Key elements include:

- The services you are providing—clearly defining scope and deliverables
- Your permitted and required uses of PHI—aligning them with the BAA to avoid conflicts
- Payment terms—including fees, billing schedules, and payment methods
- HCP warranty—ensuring the HCP has the right to disclose to you the patient PHI handled by your wearable device
- Liability limitation and indemnification—so risk is shared appropriately
- Insurance requirements—especially for costly equipment, ensuring the HCP is responsible for loss from events like fire or flood
- Fraud and abuse compliance—such as the Anti-Kickback Statute, False Claims Act, and state equivalents
- AI use and disclosure—if your device incorporates AI or the HCP uses AI in connection with the patient's visit (e.g. AI scribes), the parties should discuss how the AI tools are used and address any disclosure obligations to the patients. Transparency ensures all parties understand the potential risks and benefits of AI use by the other party or its vendors
- Informed consent and HIPAA authorization from the patients, if required—address the need, content and the method for obtaining signatures

- Coordinate with secure portal agreement (see Section III(A) below)
- Standard technology services agreement provisions, such as intellectual property protections, cybersecurity, limitations of liability, indemnification, and insurance

Careful negotiation helps avoid disputes, manage risk, and build a strong, compliant partnership with healthcare providers.

III. Internet Terms

Once your wearable device connects to the cloud and transmits patient data over the Internet, the wearable moves beyond hardware and into the realm of online services, bringing new legal requirements. At a minimum, you need three core legal documents that work together to define rights, limit liability, and address compliance obligations:

- Secure Portal Agreement—Governs HCP’s access to patient data, such as measurements and test results, through your secure online portal
- Public Website Terms of Use—Sets rules for visitors to your public site
- Website Privacy Policy—Explains data collection, use, and sharing practices

A. Secure Portal Agreement (EULA)

Staff at the physician’s office can access your wearable device results through the device’s secure, password-protected portal. That portal should have clearly drafted terms that protect your company, the data, and your intellectual property (IP), while mitigating legal risk. These terms must address HIPAA compliance and FDA regulatory considerations, as well as broader technology law issues, such as data security obligations, permitted uses of the portal, restrictions on reverse engineering or misuse, and limitations of liability.

Enforceability of portal terms depends heavily on presentation. “Terms of Use” or “Terms of Service” are often browsewrap agreements that do not require explicit assent and are harder to enforce. By contrast, an End User License Agreement (EULA) is typically a clickwrap agreement that requires users to affirmatively click “I agree” (or similar) before accessing the portal, providing stronger evidence of consent to the agreement’s terms. Clickwrap agreements provide clear evidence of consent than browsewrap terms, and are more likely to hold up in court.

Best practices for portal agreements include, among other things:

- Presenting terms as a clickwrap agreement at initial login and upon material updates
- Defining who is authorized to access the portal and for what purposes
- Specifying access rights, permitted uses, and data-sharing parameters
- Addressing ownership of portal content, data, and any derived analytics
- Tailoring disclaimers and limitations of liability
- Outlining security requirements for HCP users
- Defining account termination and data handling procedures upon contract end
- Ensuring alignment with your BAA and services agreement

B. Public Website Terms

Your public-facing website should include terms and conditions that define the rights and obligations of both the company and site visitors and limit the company's risk. Often called "Terms of Use" or "Terms of Service," these are typically structured as browsewrap agreements accessible via a link and deemed accepted when users continue to browse. However, as noted above, browsewraps are generally less enforceable than clickwrap agreements.

For websites that have a secure portal login, the public-facing web site typically uses a lighter browsewrap Terms of Use for general visitors, and the portal requires acceptance of the more robust EULA described above. The Terms of Use should also clearly reference your Privacy Policy.

Business associates should also consider the HHS's guidance on tracking technologies, and the growing wave of litigation and enforcement risk issues, which we wrote about [here](#). This is especially important for any portal that handles PHI. While less common, the public site can also trigger HIPAA obligations if it collects or transmits PHI through forms, tracking pixels, or other tools.

C. Website Privacy Policy

Your website's privacy policy must comply with FTC rules, state privacy laws and, where applicable, HIPAA requirements. HIPAA applies to business associates only when PHI is handled on behalf of a covered entity, and those obligations are usually set out in the Notice of Privacy Practices (NPP) and the BAA, not in the wearable company's website privacy policy.

FTC: The FTC actively enforces Section 5 of the FTC Act against unfair or deceptive practices. For wearable companies, this means your privacy policy must be accurate and not misleading, especially where health metrics, geolocation, or wearable data are involved. The FTC has brought numerous enforcement actions against companies for misleading privacy policies.

State law: A patchwork of state laws may apply even when HIPAA does not, including:

- Consumer privacy statutes (e.g. California Consumer Privacy Act/CPRA)
- Health data privacy laws (e.g. Washington's My Health My Data Act)
- Breach notification statutes in all 50 states
- Other rules on data collection, storage, use and sharing – including sensitive categories like biometric and neural data)

Multiple privacy policies: In response to overlapping privacy regimes, some companies now post multiple privacy policies: a general website privacy policy plus one or more health-data-specific policies where required by state law. For example, a wearable device company might maintain one standard privacy policy and a separate "Consumer Health Data Policy" for Washington residents.

Your privacy policy should clearly explain:

- What data you collect—such as health metrics, device usage, geolocation, cookies and other personal data
- How and why you collect it— including device operation, analytics, marketing, and service delivery
- Where and how the data is stored and shared— including with vendors, cloud providers, and integration partners
- Consumer choices and rights— such as access, deletion, correction, and opt-out rights (state law dependent)
- Use of tracking technologies—including analytics, pixels, and cookies, and compliance with HHS guidance on tracking tools when PHI is involved

- AI-related practices—if data will be used to train or refine AI models, disclose this in plain consumer-friendly language

Coordinate with Other Agreements: Your privacy policy should align with your public website Terms of Use and your secure portal EULA. Together, these documents form a unified framework that sets expectations for patients, healthcare providers, and other users.

A clear, comprehensive privacy policy is not only a compliance safeguard but also a business asset: it signals transparency, reduces litigation risk, and builds trust with regulators, providers, and consumers.

IV. Beyond the BAA: Using Patient Data for Analytics, AI, and Product Development

Many wearable medical device companies want to collect patient data to fuel analytics, train AI models, or support product development. If that's your goal, you must determine exactly how the data will be used, who you will share it with, and whether you have the legal rights to do so. As a BA, your use and disclosure of PHI must stay within the limits of your BAA and HIPAA. Any use outside that scope requires advance planning, careful contract review, and an understanding of applicable law. Common scenarios include:

A. Improving Your Wearable Device

- Business Associate Limitations: You may use PHI to improve device performance specifically for the HCP that supplied the data if that use is part of your defined services in the BAA. Often these uses are not covered.
- General Product Refinement: Using PHI to improve your product for other customers, or to train broadly deployed models, often exceeds standard BAA permissions. HIPAA has not been updated to address modern machine learning or AI training or refining, which leaves a spectrum of interpretations.
- To Use Wearables Data To Improve Your Device:
 - Obtain valid patient authorizations under HIPAA or
 - Use data properly de-identified under HIPAA standards.
- De-identification Considerations:
 - The BAA must explicitly allow de-identification.
 - There are two permissible methods to de-identify data under HIPAA: the Safe Harbor method and the Expert Determination method. Many companies choose the Expert Determination method so they can retain certain data elements, such as dates of service, which must be removed under Safe Harbor.

B. Supporting FDA Submissions or Research

- Wearables companies may want to use patient data collected as a BA to support clinical research or future FDA submissions. If so, they must comply with HIPAA (when PHI is involved), FDA informed consent regulations, and other research-specific rules.
- Determining when HIPAA authorizations and informed consent are required, and what each must cover, can be complex. These documents serve different purposes, and the scope of the wearable company's intended research activities is often not fully defined at the outset.
- In practice, many companies build HIPAA authorizations and informed consent into the patient workflow as an opt-in step at the time of device use.

C. Third-Party Sharing

- Wearables companies have a treasure trove of data and may think beyond their roles as business associates. Licensing de-identified datasets or allowing partners to train AI with your data requires careful legal review.
- Pay attention to HIPAA's restrictions on the sale of PHI.
- Beyond HIPAA, state health privacy laws and the FTC's Section 5 authority create additional layers of risk for secondary uses and third-party sharing.
- Review all applicable upstream and downstream contracts to ensure data-sharing is permitted and does not conflict with existing obligations.

D. Risk Mitigation and Compliance Checklist

- Confirm the HCP has the right to share the data with you.
- Align BAA language, service descriptions, and data handling workflows with actual data uses.
- Address applicable state privacy laws, FTC rules, and HIPAA.
- Adopt clear policies on tracking technologies, AI uses and disclosures, and patient rights.
- Maintain written documentation supporting your chosen de-identification method.

V. Regulatory Enforcement

Wearable medical device companies face overlapping federal and state oversight. Before finalizing agreements, it is essential to understand the key regulators and enforcement risks.

A. Key Federal Enforcement Bodies

- FDA—Regulates device safety, labeling, and marketing; its requirements may also affect contractual terms with HCPs.
- HHS Office for Civil Rights (OCR)—Enforces HIPAA and can investigate complaints and breaches involving PHI.
- FTC—Brings enforcement actions under Section 5 of the FTC Act and the Health Breach Notification Rule, in particular relating to the privacy and security of consumer health data, including misleading website privacy policies.

State Laws

In addition to federal oversight, as discussed in Section III(C) above, states are rapidly enacting consumer health data and biometric privacy laws, with neural data protections and AI-related disclosure laws gaining traction. These frameworks often apply even where HIPAA does not, creating additional compliance obligations for wearable companies. Enforcement comes from state attorneys general and, in some cases, through private rights of action.

Enforcement Convergence

A single security incident can trigger parallel investigations by multiple regulators such as OCR, FTC, the Securities and Exchange Commission (SEC), and state attorney generals, in addition to private litigation and shareholder claims.

VI. Conclusion

Wearable health technology is no longer a niche—it's a core driver of healthcare innovation. With that visibility comes heightened scrutiny. Federal and state agencies are sharpening their focus on how companies collect, use, and share health data, with enforcement extending into AI, biometrics and consumer health privacy.

Takeaway: Embed compliance and contractual protections into your wearable device and operations from the outset. A proactive approach not only reduces regulatory and litigation risk, but also strengthens trust and market credibility needed for sustained growth.

The author would like to thank Bannie Bajwa for her contribution to this post.



If you have any questions or would like more information about these developing issues, please contact the following:

KATHERINE LEIBOWITZ
1-610-896-5788
Katherine.Leibowitz@LeibowitzLawTeam.com