

FDA's 2026 Guidance on General Wellness Devices: Policy for Low-Risk Devices

WRITTEN BY

Kyle A. Dolinsky | Karla Ballesteros | Kaitlin J. Clemens | Samarth Parikh

This three-part series reviews how the Food and Drug Administration's (FDA) January 2026 guidance, "General Wellness: Policy for Low Risk Devices"^[1] (the General Wellness Guidance), affects companies offering "wellness tracker" products.

The General Wellness Guidance may leave some organizations questioning when a wellness tracker is an FDA-regulated "device" as opposed to a general wellness product outside the scope of FDA regulation but subject to other legal risks. Part Two of our series distills the General Wellness Guidance into four key takeaways:

1. FDA will not regulate low-risk general wellness products as devices.

Low-risk general wellness products either fall outside the definition of "device" entirely, or FDA will exercise enforcement discretion. Whether your product is regulated as a device depends on its intended use, judged objectively from labeling, marketing, and other statements, and whether it is "low-risk" as defined in the General Wellness Guidance.

2. Noninvasive physiologic trackers may now qualify as general wellness products.

The 2026 update to the General Wellness Guidance indicates that certain noninvasive products measuring physiologic parameters (like blood pressure) can be treated as general wellness products if they are truly intended for wellness use and avoid diagnostic or treatment claims.

3. You can tell users to talk to a doctor — within narrow limits.

General wellness products may prompt users to consult a health care professional when outputs fall outside normal thresholds, so long as they do not make disease-specific, diagnostic, or treatment-oriented statements.

4. FDA cybersecurity rules may not apply — but privacy and security obligations still do.

Because they are not regulated as devices, low-risk general wellness products do not have to comply with the requirements of FDA's 2026 guidance, "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions"^[2] (Cybersecurity Guidance).^[3] However, as covered in [Part One](#), they may still be subject to HIPAA and other federal and state privacy and security laws, and they still present meaningful cybersecurity and incident response risk.

I. FDA will not regulate low-risk general wellness products as devices.

The General Wellness Guidance revises and replaces a 2019 guidance published under the same title but keeps the same core position: low-risk general wellness products are subject to enforcement discretion and will *not* be regulated as devices under the federal Food, Drug, and Cosmetic Act (FDCA).^[4] The General Wellness Guidance thus addresses two key questions: (1) whether a product is a "general wellness product"; and (2) whether it is low-risk.

In determining whether a product is a general wellness product, the General Wellness Guidance continues to

focus on the product's intended use: it must be intended either for (1) a use that relates to maintaining or encouraging a general state of health or a healthy activity, or (2) a use that relates the role of a healthy lifestyle with helping to reduce the risk or impact of certain chronic diseases or conditions and where it is well understood and accepted that healthy lifestyle choices may play an important role in health outcomes for the disease or condition.

To determine whether a general wellness product is low risk, FDA considers whether a product is invasive, implanted, or contains technology that poses a safety risk without specific regulatory controls. If so, the product will not be considered low risk, and the General Wellness Guidance will not apply. This approach has not changed from the 2019 version of the General Wellness Guidance.

II. Noninvasive physiologic trackers may now qualify as general wellness products.

The most significant change in the 2026 General Wellness Guidance compared to the 2019 version concerns products used to sense, estimate, infer, or output physiologic parameters (such as blood pressure, oxygen saturation, blood glucose, and heart rate variability). Whereas the 2019 version of the General Wellness Guidance was silent as to these products, the 2026 update clarifies that these products may be general wellness products if they are intended solely for wellness use *and* they:

- Are noninvasive.
- Do not involve technology that poses a safety risk.
- Are not intended for diagnosis, cure, mitigation, prevention, or treatment of a disease.
- Are not intended to substitute for an FDA-approved or FDA-cleared device.
- Do not include claims, functionality, or outputs that guide clinical management.
- Do not include values that mimic those used clinically, unless validated.

In determining that products measuring physiologic parameters can qualify as general wellness devices, FDA has appeared to change its approach from as recently as last year. In July 2025, FDA sent a warning letter to a wearable product manufacturer for its blood pressure insights functionality, stating that blood pressure measurements are inherently associated with hypo- and hypertension diagnoses, and thus the manufacturer's product was not a general wellness product and would require prior FDA approval or clearance.^[5] Then, in September 2025, FDA released a safety communication stating that blood pressure measuring devices "are required to receive FDA marketing authorization to be lawfully marketed in the United States" and "do not fall within the FDA's policy for general wellness products because they are not intended solely for general wellness use and are not low risk."^[6] Whereas its 2025 communications suggest that blood pressure measuring devices categorically could not qualify as general wellness products, the 2026 updated General Wellness Guidance states that they can.

In changing course, FDA appears to be adhering more faithfully to its policy by focusing on the intended use of a potential general wellness product. Importantly, though, FDA has always determined, and continues to determine, a product's "intended use" based on an objective standard.^[7] FDA will look to a firm's regulatory filings, product labeling, advertising and promotion, and any other statements as indicative of a product's intended use. While the updated General Wellness Guidance states that blood pressure measuring products are not categorically excluded from general wellness products, it is still possible that, under the circumstances, the product at issue in

FDA's July 2025 warning letter would not qualify as a general wellness product and would require marketing authorization. Therefore, companies must diligently monitor all statements about their products to ensure their objectively intended use matches what the company in fact intends.

III. You can tell users to talk to a doctor — within narrow limits.

The updated General Wellness Guidance clarifies that products may inform users to consult a health care professional when outputs fall outside normal thresholds and still qualify as general wellness products if the following conditions are met:

- Notifications make no reference to a specific condition or disease.
- Outputs are not categorized as abnormal, pathological, or diagnostic.
- No recommendations are included concerning clinical thresholds, diagnosis, or treatment.
- No ongoing monitoring or alerts for medical management are provided.

FDA differentiates between these kinds of alerts and ongoing monitoring or treatment recommendations that indicate a product is intended for something other than general wellness use.

New Examples

The 2019 version of the General Wellness Guidance provided six examples to illustrate when general wellness products would not be considered devices or would be subject to enforcement discretion. The 2026 update provides three additional examples to help illustrate application of the General Wellness Guidance to products that measure physiologic parameters:

New Example 7: A wrist-worn wearable product intended to assess activity and recovery that outputs multiple biomarkers like hours slept, sleep quality, pulse rate, and blood pressure using noninvasive technology.

New Example 8: A wearable product intended to provide blood glucose estimations for monitoring nutritional impacts using a minimally invasive microneedle technology.

New Example 9: A noninvasive wearable product intended for monitoring electrolyte imbalance, lactate, and hemoglobin. This product is advertised toward elite athletes and is labeled for use in an exercise/fitness context only and disclaims for use diagnosing any condition.

According to the General Wellness Guidance, both the products in examples 7 and 9 would be considered low-risk general wellness products because they do not refer to a specific disease or condition and the noninvasive technologies do not pose a safety risk. These examples reflect a shift in FDA's position because as described above, devices that measure certain physiologic parameters like blood pressure would have required marketing authorization under FDA's prior practice. In contrast to examples 7 and 9, example 8 would not be a low-risk general wellness product because even minimally invasive technology is "invasive" and thus not low risk.^[8]

IV. FDA cybersecurity rules may not apply — but privacy and security obligations still do.

In February 2026, FDA issued its Cybersecurity Guidance, superseding 2025 and 2023 final guidances. Under the 2026 requirements, manufacturers must design, develop, and maintain processes that provide “reasonable assurance” of cybersecurity, including post-market updates, patches, and a plan to monitor, identify, and address vulnerabilities. FDA interprets this requirement to mean that manufacturers should provide a detailed cybersecurity management plan (CMP) as part of the premarket submission for cyber devices.^[9] FDA intends to review the CMP as part of its safety and effectiveness review, treat cybersecurity risks like any other safety risk, and may reject premarket submissions that do not provide adequate information or a “reasonable assurance” of cybersecurity.

However, as discussed above, the General Wellness Guidance removes low-risk general wellness products from the scope of FDA regulation. Because FDA determined that low-risk general wellness products are not regulated as devices, these products will not be subject to premarket and post-market regulatory requirements under the FDCA. Even if FDA regulations do not apply, significant privacy, security, regulatory, and litigation risks still exist.

As discussed in the first article of this series, the Federal Trade Commission (FTC) has actively pursued enforcement actions against manufacturers of general wellness products that fail to implement reasonable security measures. In addition, sector-specific health laws may apply when a general wellness product integrates with covered entities (e.g., health care providers or health plans). In those circumstances, the manufacturer may become a “business associate” and be subject to HIPAA’s security requirements.

Manufacturers must also navigate a patchwork of state laws, as all 50 states and U.S. territories impose data breach notification obligations. While security measures are not always explicitly required by statute, building in robust security significantly benefits companies given these universal notification requirements. Finally, inadequate security can give rise to product liability and other litigation risks, including claims alleging negligence in data security and harm resulting from a breach — with an increased likelihood of class action exposure following data incidents.

The General Wellness Guidance means that many wellness trackers can avoid device-level cybersecurity obligations — but not cybersecurity risk. In the third and final article in this series, we will turn to those risks directly and walk through practical cybersecurity and incident response considerations for wellness tracker companies.

[1] U.S. Food & Drug Admin., *Guidance for Industry: General Wellness: Policy for Low Risk Devices*, (Jan. 2026), <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices>.

[2] U.S. Food & Drug Admin., *Guidance for Industry: Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions*, (Feb. 2026), <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions>.

[3] During the publication process of Part One of our series, FDA issued a new version of the cybersecurity guidance, superseding its June 2025 version. The new cybersecurity guidance is substantially the same but replaces references to Quality System (QS) with Quality Management System Regulation (QMSR), placing greater emphasis on risk management throughout the product lifecycle.

[4] The term “device” is defined in 201(h) of the FD&C Act to include an “instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is ...intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man ... or intended to affect the structure or any function of the body of man...” and “does not include software functions excluded pursuant to section 520(o) of the FD&C Act.”

[5] <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/whoop-inc-709755-07142025>.

[6] <https://www.fda.gov/medical-devices/safety-communications/do-not-use-unauthorized-devices-measuring-blood-pressure-fda-safety-communication>.

[7] See 21 C.F.R. § 801.4; see also <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/whoop-inc-709755-07142025>.

[8] The General Wellness Guidance defines “invasive” as “penetrates or pierces the skin or mucous membranes of the body.” General Wellness Guidance at 6 n.9.

[9] Section 524B of the FDCA defines “cyber device” as a device that meets all of the following criteria (1) includes software validated, installed, or authorized by the sponsor as a device or in a device; (2) has the ability to connect to the internet; and (3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats.

RELATED INDUSTRIES + PRACTICES

- [Data + Privacy](#)
- [FDA Regulatory + Risk Management Counseling](#)
- [Health Care + Life Sciences](#)
- [Privacy + Cyber](#)