Articles + Publications | February 19, 2026

Wellness Trackers, ‘Medical’ Status, and Cybersecurity: How FDA, FTC, and State Laws Interlock

WRITTEN BY

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

On January 6, 2026, the Food and Drug Administration (FDA) issued its *General Wellness: Policy for Low Risk Devices*[1] guidance (the General Wellness Guidance), signaling that it does not intend to enforce traditional medical device requirements for “general wellness products,” including many wearables and apps that promote healthy lifestyle goals. As a result, wellness trackers that qualify as general wellness products will not face the same premarket scrutiny or presubmission cybersecurity expectations that apply under FDA’s June 2025 guidance, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* (the Cybersecurity Guidance).[2] But the absence of FDA oversight does not make these technologies low risk: whether regulated devices or general wellness products, they collect large volumes of sensitive data and remain attractive targets for threat actors, with common security weaknesses leading to unauthorized access, extortion, and fraud.

General wellness products also sit at the intersection of overlapping regulatory regimes. HIPAA applies only when an entity is a “covered entity” or “business associate,” a category many wellness?tracker developers do not meet. FDA requirements apply when a product qualifies as a “medical device.” Even when FDA exercises enforcement discretion, the Federal Trade Commission’s (FTC) Health Breach Notification Rule (HBNR) and a growing patchwork of state data breach and privacy laws continue to govern the collection, use, and unauthorized access of health and wellness information.

This article is the first in a three?part series: Part One surveys the overlapping frameworks (HIPAA, HBNR, and key state laws); Part Two examines FDA’s General Wellness Guidance; and Part Three addresses incident response and why organizations still need robust cybersecurity and response capabilities.

The Interlocking Frameworks for General Wellness Products

1) FDA’s Cybersecurity Guidance and Its Applicability to General Wellness Products

In June 2025, FDA issued its final Cybersecurity Guidance superseding its 2023 final guidance on cybersecurity in medical devices. The updated guidance clarifies compliance expectations for “cyber devices”[3] under Section 524B of the federal Food, Drug, and Cosmetic Act (FDCA), which requires manufacturers to design, develop, and maintain processes that provide “reasonable assurance” of cybersecurity, including postmarket updates, patches, and a plan to monitor, identify, and address vulnerabilities.[4] The Cybersecurity Guidance incorporates these requirements into Quality System requirements and advises manufacturers to address them in a Cybersecurity

Management Plan (CMP) submitted with their premarket submissions. The CMP should include the following elements:

- Personnel responsible;
- Sources, methods, and frequency for monitoring and identifying vulnerabilities;
- Identification and addressing of vulnerabilities identified by the Cybersecurity and Infrastructure Security Agency;
- Periodic security testing;
- Timeline to develop and release patches;
- Update processes;
- Patching capability;
- Description of coordinated vulnerability disclosure process; and
- Description of how the manufacturer intends to communicate forthcoming remediations, patches, and updates to customers.

FDA will 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.

The General Wellness Guidance identifies certain would-be devices as "general wellness products," which FDA views as falling outside the FDCA definition of "device"[5] and therefore outside FDA regulation. The General Wellness Guidance provides a two-part definition for general wellness devices. To qualify, a product must (1) be intended only for general wellness use (such as maintaining or encouraging a general state of health, or supporting healthy lifestyle choices that are well?accepted to reduce the risk or impact of certain chronic diseases or conditions), and (2) present a low risk to user safety. Products that do not meet both criteria are treated as devices subject to FDA oversight.

Because FDA has determined that general wellness products fall outside its regulatory scope, they are not subject to the FDCA's premarket or postmarket requirements, including the extensive obligations in the Cybersecurity Guidance.

2) HIPAA's Breach Notification Rule

a) Who Does It Govern?

FDA's General Wellness Guidance signals that general wellness products will not be regulated as medical devices, but they still sit within the broader health privacy ecosystem. HIPAA and its HBNR still govern "covered entities" (such as health plans, most health care providers conducting standard electronic transactions, and health care clearinghouses) and their "business associates" (service providers that handle protected health information (PHI) on behalf of a covered entity for those entities, such as IT, cloud providers, billing or analytic providers). Business associates are directly regulated under HIPAA with respect to the PHI they handle and must notify the covered entity when they discover a breach. Thus, even if FDA does not treat a general wellness product as a device, its manufacturer or operator qualifies as a HIPAA business associate when it receives, creates, maintains, or transmits PHI on behalf of a covered entity — for example, a cardiac monitoring platform that stores and

analyzes identifiable heart rhythm data for clinicians under a Business Associate Agreement (BAA).

b) What Types of Information Does It Govern?

FDA's interpretation that general wellness products are not regulated devices does not alter HBNR, which continues to strictly protect PHI when these products are used in clinical or plan-sponsored settings. PHI is individually identifiable health information held or transmitted by a covered entity or business associate in any form — electronic, paper, or oral — that relates to an individual's past, present, or future physical or mental health or condition, the provision of care, or payment for care, and that includes identifiers that can reasonably be used to identify the person. Identifiers range from names and Social Security numbers to combinations of dates, addresses, or device identifiers that can be tied back to an individual. If data from a general wellness product is integrated into a provider's record system or plan platform in a way that meets this definition, it becomes PHI, regardless of FDA's enforcement posture. Properly de?identified data, where the risk of reidentification is very low, falls outside HIPAA and HBNR.

3) TC Health Breach Notification Rule

FDA's General Wellness Guidance removes device?level oversight for general wellness products, but the FTC's HBNR is designed to catch exactly the kind of consumer health apps and wearables that fall outside HIPAA. Adopted in 2009, HBNR applies to entities that handle personal health records that are not PHI under HIPAA and functions as a "catch-all" breach rule for health apps, wellness trackers, and connected devices that are not operating as HIPAA covered entities or business associates. The FTC's 2021 policy confirmed that health apps and connected devices that collect or use consumers' health information must comply with HBNR, and 2024 amendments clarified that the Rule expressly covers personal health information in health apps, fitness trackers, and other wearable devices — precisely the products FDA is now treating as low?risk general wellness products.

For example, in May 2023, the FTC charged a fertility app developer with violating the FTC's HBNR by secretly sharing users' sensitive health information with third parties without adequate encryption. Under a proposed order, the app developer agreed to pay a $100,000 civil penalty.[6]

a) Who Does It Govern?

In the wake of FDA's January 6 guidance, many general wellness product companies may not see themselves as "medical device manufacturers," but they may still be squarely covered by HBNR. The rule applies to foreign and domestic vendors of personal health records (PHRs), PHR?related entities, and third?party service providers that maintain information about U.S. residents, while explicitly excluding HIPAA covered entities and entities insofar as they act as business associates.[7] In practice, if a wellness tracker or app that qualifies as a general wellness product maintains electronic health information about an individual and can draw that information from multiple sources, its provider is likely a PHR vendor or related entity.[8] That means the shift away from FDA medical?device oversight does not eliminate legal exposure — HBNR becomes the primary breach?notification framework for many wellness trackers.

b) What Types of Information Does It Govern?

HBNR covers “PHR identifiable health information” in PHRs and related services that fall outside HIPAA, which closely aligns with data collected by modern wellness trackers. This includes individually identifiable health information (*e.g.*, conditions, treatments, biometrics, reproductive and genetic data, symptoms, and other health measurements) created, received, or stored by a PHR vendor, PHR?related entity, or third?party service provider, particularly when drawn from multiple sources such as apps, devices, or websites.[9] Because many wellness trackers aggregate data from wearables, phones, and third?party services, they may qualify as general wellness products for FDA purposes, but HBNR still treats unauthorized disclosures of their data as “breaches” that trigger legal obligations.

4) State Data Breach and Privacy Laws

FDA’s General Wellness Guidance clarifies that FDA will not regulate general wellness products as devices, but it does not affect state data breach and privacy laws, which often protect the same health data these products collect. State breach notification laws generally apply to entities that own, license, maintain, or otherwise handle residents’ “personal information,” regardless of whether they are traditional health care providers or FDA?regulated device manufacturers. This includes wellness app developers, wearable manufacturers, fitness platforms, menstrual or fertility tracking apps, and other consumer?facing technology companies that collect or analyze health?related data. As a result, even if wellness trackers qualify as general wellness products and fall outside FDA device regulation, they may still face significant cybersecurity and notification obligations under state law.

For example, in September 2020, a fertility-tracking app entered into a stipulated judgment with the California Department of Justice over alleged violations of California medical privacy and data security laws. The app collected highly sensitive sexual and reproductive health information but allegedly had basic security vulnerabilities and failed to recognize its obligations under the Confidentiality of Medical Information Act (CMIA), which extends beyond federal law to cover health apps. As part of the settlement, the company agreed to pay $250,000.[10]

a) Who Do They Govern?

State data breach statutes generally focus not on whether a product is an FDA?regulated device, but on whether an entity holds covered “personal information” about state residents. This brings many wellness?tracker companies within scope, even if they view themselves as lifestyle or consumer tech rather than health care providers. So, while FDA may not impose pre-market cybersecurity obligations on general wellness products, state attorneys general and other regulators can still enforce state breach and privacy laws if these trackers mishandle covered data.

b) What Types of Information Does It Govern?

Many state breach statutes define “personal information” to include medical information, health insurance information, and biometric data — categories that closely track what wellness trackers collect. “Medical” or “health” information often covers an individual’s medical history, physical or mental condition, or treatment, while “biometric data” includes identifiers like fingerprints, facial recognition, or iris scans used by some wearables. As a result, data from consumer tools that infer health conditions (*e.g.*, depression), estimate metrics (*e.g.*, blood pressure, sleep), or track reproductive or sexual health may qualify as protected medical or health information

under state law, even if FDA classifies them as "general wellness products." In addition, several states (including California, Washington, Colorado, Connecticut, and Virginia) have comprehensive privacy laws that treat health data as "sensitive," imposing heightened requirements on its collection, use, and sharing.

***

For organizations developing or deploying wellness apps, partnering with outside counsel can help ensure you address the full multilayered regulatory landscape.

In Part Two of this series, we will take a closer look at FDA's General Wellness Guidance and how companies can position their products in light of FDA's current enforcement posture.

---

[1] General Wellness: Policy for Low Risk Devices | FDA

[2] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions | FDA

[3] 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.

[4] 21 U.S.C. § 360n-2(b).

[5] 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."

[6] Federal Trade Commission, *Ovulation Tracking App Premom Will Be Barred from Sharing Health Data for Advertising Under Proposed FTC Order* (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc.

[7] Id.

[8] FTC, *Complying with the FTC's Health Breach Notification Rule*; FTC Rule overview; 16 C.F.R. § 318.1(a).

[9] 16 C.F.R. § 318.2

[10] California Office of the Attorney General, *Attorney General Becerra Announces Landmark Settlement Against Glow Inc. – A Fertility-Tracking App That Mishandled Users' Sensitive Health Information* (press release), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- FDA Regulatory + Risk Management Counseling
- Health Care + Life Sciences
- Privacy + Cyber