Articles + Publications | April 21, 2026

Outside FDA, Inside the Crosshairs: Cybersecurity Risks for General Wellness and Fitness Products

WRITTEN BY

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

In Part One of this series, we discussed how wellness products sit at the intersection of Food and Drug Administration (FDA), Health Insurance Portability and Accountability Act (HIPAA), Federal Trade Commission (FTC), and state privacy/breach laws. In Part Two, we analyzed FDA's 2026 General Wellness guidance and what it means for device-level cybersecurity expectations. In this final installment, we focus on the cybersecurity risks and legal obligations that apply even when a product qualifies as a low-risk general wellness product and falls outside FDA's premarket cybersecurity requirements.

I. No FDA Regulation, Same Level of Scrutiny

As discussed in Part Two, FDA's January 2026 guidance, *General Wellness: Policy for Low Risk Devices*, confirms that low-risk "general wellness products" (as categorized based on their intended use) fall outside active FDA device regulation.

As Part One noted, the absence of FDA oversight does not eliminate regulatory risk. General wellness products still often collect sensitive, identifiable information and, as a result, may be subject to heightened cybersecurity and privacy scrutiny under the FTC's Health Breach Notification Rule (HBNR), HIPAA, and state privacy and breach-notification laws. The sections below address each framework, when it may apply, and how they intersect. Because these regimes do not operate in isolation, developers must track and meet the distinct timelines and requirements under each.

II. FTC's HBNR: A Potential Pitfall for Developers

The FTC's HBNR applies to entities that are not subject to HIPAA but handle unsecured, personally identifiable health information, including personal health record (PHR) vendors, related health apps and devices, and their service providers. Developers of general wellness products, including apps, can become PHR vendors when their products aggregate health information from multiple sources or allow users to input or sync data from other services. In 2021, the FTC underscored HBNR's reach to health apps, noting that as consumers increasingly use apps to track conditions, treatments, fitness, fertility, sleep, mental health, diet, and other health data, the rule "is more important than ever."[1] The FTC even released a tool for mobile health app developers to use to see which regulations apply: Mobile Health App Interactive Tool | Federal Trade Commission.

a. When does it apply to general wellness products?

Many developers of general wellness products do not see themselves as PHR vendors, instead viewing their products as consumer fitness or lifestyle tools. But marketing choices and integrations — such as syncing with provider portals, connecting to wearables, or collecting geolocation data via application programming interfaces (APIs) — can mean they are aggregating health information from multiple sources. When these tools are primarily managed by or for an individual, they can qualify as PHRs and fall under FTC oversight, whether or not developers recognize it.

Importantly, the HBNR itself does not prescribe a detailed cybersecurity framework (for example, specific encryption standards, access control models, or testing regimes). Instead, it creates breach-notification obligations that sit alongside, and are informed by, the broader "reasonable security" expectations that FTC has articulated through enforcement actions under Section 5 of the FTC Act.

b. Obligations under FTC's HBNR

Under the HBNR, obligations are triggered when a covered entity experiences an unauthorized acquisition of unsecured, identifiable health information in a PHR due to a data breach or unauthorized disclosure. Importantly, this is not limited to just when someone accesses an organization's systems in a cybersecurity incident. It also includes when a business shares covered information without an individual's authorization. When such a breach of security occurs, HBNR requires the covered entity to:

- Notify the affected individuals whose information was compromised;
- Notify FTC; and
- If more than 500 individuals in a particular jurisdiction are affected, notify appropriate media outlets.

Failure to comply can result in civil penalties.

c. "Reasonable Security": No Explicit Standard, But a Clear Message from Enforcement

The HBNR itself does not prescribe specific cybersecurity controls. Instead, the operative framework comes from the FTC's Section 5 authority, which prohibits "unfair or deceptive" practices and effectively requires "reasonable" security for sensitive health data — a flexible, context-dependent concept.

Recent FTC actions involving general wellness products offer practical guidance. The FTC has alleged Section 5 violations where companies:

- Failed to implement basic security safeguards proportionate to the sensitivity of health data; and
- Misrepresented or overstated their security and privacy protections.

Patterns in these cases include criticism of:

- Weak access controls and authentication;
- Inconsistent or inadequate encryption;
- Poor oversight of third-party software development kits (SDKs) and tracking tools that exposed health information; and

- Privacy policies and marketing that promised stronger protections than were actually in place.

Taken together, HBNR and related enforcement show that compliance is more than issuing breach notices. Businesses should ensure their security programs match the sensitivity and volume of the data they collect and that public statements accurately reflect their practices. Developers of health and wellness apps that qualify as general wellness products should treat HBNR as part of a broader risk and compliance framework, using FTC "reasonable security" guidance in health and digital services cases to inform both technical safeguards and consumer-facing disclosures.

III. HIPAA: When Wellness Products Enter the Health Care Ecosystem

In Part 1, we explained that HIPAA and its Breach Notification Rule apply to "covered entities" (health plans, most providers conducting standard electronic transactions, and clearinghouses) and their "business associates" (service providers that handle PHI, such as IT vendors, cloud providers, billing, and analytics firms). It also encompasses health information in any form (electronic, paper, or oral) that can be linked to an identifiable individual and relates to that person's past, present, or future physical or mental health, care received, or payment for that care. Once an organization is handling PHI in that capacity, HIPAA's cybersecurity requirements are triggered, with a particular focus on electronic PHI (ePHI).

a. When does it apply to general wellness products?

Wellness products and health apps that otherwise qualify as general wellness products may still fall within HIPAA's cybersecurity framework when they handle PHI on behalf of covered entities. For example, an app that collects, stores, or transmits identifiable health information for a hospital or health plan pursuant to a Business Associate Agreement (BAA) is acting as a business associate and must comply with the Security Rule's safeguard requirements and the Breach Notification Rule's incident-response obligations.

In that role, the app developer is not merely offering a consumer-facing tool; it is operating within the covered entity's regulated environment. That status carries specific cybersecurity responsibilities, including implementing appropriate safeguards for ePHI and maintaining breach response procedures that enable the covered entity to meet its notification requirements.

When HIPAA applies, the FTC's HBNR generally does not. Section 5 of the FTC Act, however — which prohibits unfair or deceptive acts or practices — continues to govern the company's representations about its privacy and security practices and the adequacy of its data security measures.

b. Cybersecurity-Related Obligations under HIPAA's Breach Notification Rule

The HIPAA Breach Notification Rule complements the Security Rule by imposing obligations when security incidents occur. Covered entities and business associates must assess potential breaches of unsecured PHI and, where a breach is determined, provide timely notice.

Covered entities are required to notify affected individuals and the U.S. Department of Health and Human Services secretary without unreasonable delay, and no later than 60 days after discovery of a breach. Business associates,

in turn, must notify the relevant covered entity without unreasonable delay and within the same 60?day outer limit.

Although the Breach Notification Rule is not itself a security framework, it reinforces the need for effective detection, investigation, and response capabilities, as organizations must be able to identify incidents involving PHI, evaluate risk, and carry out required notifications.

c. Cybersecurity Obligations under HIPAA's Security Rule

Under the HIPAA Security Rule, covered entities and business associates must protect ePHI through a coordinated set of administrative, physical, and technical safeguards. In practice, this requires organizations to establish a formal security program that, at a minimum, includes:

- Conducting regular and thorough risk analyses to identify threats and vulnerabilities to ePHI;
- Implementing risk management measures and security policies to address identified risks;
- Training workforce members on security responsibilities and acceptable use;
- Enforcing role-based access controls and authentication to limit access to ePHI;
- Implementing technical safeguards such as unique user IDs, audit controls, and integrity protections;
- Considering the use of encryption for ePHI in transit and at rest, and documenting decisions where encryption is not implemented; and
- Executing BAAs that require vendors to apply appropriate security safeguards to ePHI.

The Security Rule is intentionally flexible and scalable, but it expects organizations to match their safeguards to the nature of their systems and the sensitivity and volume of ePHI they handle.

IV. Other Emerging State-Law Obligations

a. State Privacy Laws

A growing number of comprehensive state privacy laws — including in California, Colorado, Connecticut, Virginia, and others — treat health data (and in some cases "precise geolocation related to health visits") as sensitive personal information. They generally require data minimization and purpose limitation, heightened consent (especially for secondary uses), stronger security safeguards, and expanded rights to access, delete, restrict processing, or opt out.

Some states go further by adopting targeted protections for reproductive and other sensitive health data. For a state-by-state breakdown, see our article on how state laws fill gaps left by HIPAA in this area.

This is particularly significant for developers of wellness and lifestyle apps and devices that qualify as general wellness products, which, although not traditional medical devices, can detect highly sensitive health information from user inputs, sensor data, location, and usage patterns.

b. State Cybersecurity Audit Requirements

States are also beginning to impose comprehensive cybersecurity audit requirements on certain businesses,

mandating formal assessments and submission of results to regulators. For example, under the California Consumer Privacy Act (CCPA), the California Privacy Protection Agency requires certain businesses to conduct annual cybersecurity audits and certify compliance. For more detail on CCPA's cybersecurity audit requirements, please see our five-part article series. Developers of general wellness products may fall within the scope of these audit obligations without realizing it.

V. What Now?: Cybersecurity for Wellness Products Beyond FDA Oversight

Ultimately, there is no such thing as "perfect security," and none of the major legal frameworks prescribe a foolproof path. Instead, they converge around a "reasonable security" framework, under which an organization's safeguards are evaluated considering its size, the nature and volume of data collected, and the robustness of its controls. For developers of general wellness products, this means treating wellness data as highly sensitive and building security into every stage of the product lifecycle — from design and development through deployment and maintenance.

In practice, this includes mapping and documenting data flows, classifying data by sensitivity (*e.g.*, health metrics, location, biometrics, and inferences), conducting regular security risk assessments that account for the FTC's HBNR, HIPAA's Breach Notification Rule, and state privacy and breach laws, and testing incident response (*e.g.*, via tabletop exercises). As features, partnerships, and market footprints change, developers should reassess their regulatory posture and update their programs. The absence of FDA pre-market cybersecurity obligations does not create a safe harbor; the FTC's enforcement authority, HIPAA, and an expanding network of state privacy and security laws — including the CCPA – collectively impose stringent expectations that must be integrated into any cybersecurity and compliance strategy.

---

[1] statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

RELATED INDUSTRIES + PRACTICES

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