akerman

Blog Post

Fitbits at Work: Navigating the Legal Risks of Wearables in Corporate Wellness Programs

June 26, 2025
By M. Adil Yaqoob

At a time where personal fitness devices track everything from heart rate to sleep quality, employers are increasingly integrating wearable technology — like Fitbits, Apple Watches, and Oura Rings — into their corporate wellness programs. These programs promise to reduce healthcare costs, boost productivity, and foster a culture of well-being. But with these benefits come significant potential legal pitfalls, particularly in the areas of data privacy, HIPAA, and disability discrimination.

Biometric Data and Privacy Laws

The data collected by wearables often qualifies as *biometric information* — a category of sensitive personal data that includes heart rate, sleep cycles, skin temperature, and oxygen saturation levels. While there is no comprehensive federal biometric privacy law, a state like Illinois (with the Biometric Information Privacy Act, or BIPA) imposes strict requirements on entities collecting such data.

Employers operating in Illinois must provide written notice, obtain informed consent, and maintain publicly available policies on data retention and destruction. Violations, even if inadvertent, can carry steep statutory damages — up to $5,000 per violation.

Related People

M. Adil Yaqoob

Related Work

Data Privacy and Security
Employment Administrative Claims Defense
Employment Training and Compliance
Labor and Employment

Related Offices

New York

HR Defense

Akerman Perspectives on the Latest Developments in Labor and Employment Law

Visit this Akerman blog

Employers should consider whether they, or third-party wellness vendors, are collecting and storing biometric data in a way that triggers state law obligations. Even if an employer doesn't *touch* the data directly, liability may attach if the program is employer-sponsored.

HIPAA

A common misconception is that any health-related data is protected by the Health Insurance Portability and Accountability Act (HIPAA). In reality, HIPAA only applies to covered entities (like healthcare providers and insurers) and their business associates.

If a wellness program is not in connection with the employer's group health plan, HIPAA will likely not apply. But if the program is integrated with an employer-sponsored health plan or if incentives are tied to group health insurance premiums, HIPAA obligations likely kick in.

Employers should also be cautious about accessing individualized data. If an HR department reviews a dashboard showing an employee's elevated heart rate, that might not just be a HIPAA issue — it could implicate disability discrimination laws as well.

ADA Compliance

The Americans with Disabilities Act (ADA) places strict limits on when and how employers may conduct "medical examinations" or make "disability-related inquiries." The EEOC has interpreted this to include wellness programs that require employees to divulge health information — even voluntarily — if substantial incentives are attached.

In 2017, the EEOC's rules on wellness program incentives were vacated, leaving employers with limited guidance on what constitutes a "voluntary" program. A wearable-based initiative that offers large financial incentives or penalizes employees for opting out may not pass muster under the ADA.

Moreover, employers who receive individualized biometric data may face ADA claims if they use that information to make employment decisions, even inadvertently.

Best Practices for Employers

To mitigate risk while still reaping the benefits of wearable-integrated wellness programs, employers should consider the following:

1. **Vet Vendors Carefully**: Ensure third-party wellness vendors have robust privacy and data security practices and indemnify employers for legal risks.
2. **Obtain Informed Consent**: For jurisdictions with biometric privacy laws, provide clear notice and obtain written consent before collecting any data.
3. **Keep It Voluntary**: Ensure participation is truly optional and avoid large incentives or penalties that could make the program coercive.
4. **Avoid Accessing Individual Data**: Aggregate data is less risky than individualized metrics. If individual data is accessed, HR and management should be trained on anti-discrimination obligations.
5. **Coordinate With Legal and Compliance**: Involve counsel early in the design and implementation process to ensure HIPAA, ADA, and state law compliance.

Reaching the Finish Line

Wearable technology can be a powerful tool for promoting employee health, but it's not a risk-free endeavor. Employers must tread carefully to ensure that their wellness initiatives don't inadvertently violate biometric privacy laws, HIPAA, or the ADA. As always, good intentions are no defense to a poorly designed program that runs afoul of the law. For guidance on adapting to the developing legal landscape of wearables in the workplace, consult your Akerman Labor and Employment attorney