FEBRUARY 7, 2025 | AI/TECHNOLOGY, PRIVACY & DATA SECURITY

The EEOC's New Guidance on Wearable Tech: What Employers Need to Know

BY DARIUS ROHANI-SHUKLA & JORDAN B. SCHWARTZ

By Darius Rohani-Shukla and Jordan B. Schwartz

Last year, many of our clients began asking us about the feasibility of requiring or, at the very least, providing their employees with the option of using "wearable technology" in the workplace. As wearable technologies become increasingly integrated into workplace operations, the Equal Employment Opportunity Commission (EEOC) has issued new guidance outlining how these innovations intersect with employment discrimination laws. The guidance is consistent with the advice and counsel we have been providing on this issue, including the concern that requiring workers to use wearable devices, without adequate legal safeguards, could expose a company to liability. While these devices—ranging from smartwatches to biometric scanners—offer potential benefits in efficiency, safety, and health monitoring, employers embracing these tools must navigate a landscape shaped by federal laws like the Americans with Disabilities Act (ADA), the Genetic Information Nondiscrimination Act (GINA), and Title VII of the Civil Rights Act.

Key Considerations from the EEOC's Guidance

The EEOC's fact sheet and accompanying guidance highlight several areas where wearable technologies may run afoul of anti-discrimination laws. Below are the primary concerns that employers should consider:

1. **Potential for Disability Discrimination (ADA)**

Wearables that track biometric data such as heart rate, oxygen levels, or stress indicators can inadvertently reveal medical conditions and may be considered a medical examination or a disability-related inquiry under the ADA. If employers use this information to make employment decisions—whether intentionally or not—they risk violating the ADA, which prohibits discrimination based on disability and mandates reasonable accommodations.

Employer Tip:

Companies should establish clear policies ensuring that health data collected through wearables is not used to make adverse employment decisions unless doing so is specifically job-related and consistent with business necessity and/or safety. Accordingly, employers should utilize checks and balances to ensure that any adverse employment decisions are not made in haste based on data gleaned from wearable technology. To the extent that your company chooses to collect information and/or data about an employee's physical or mental condition

from wearable devices, you should treat such data as confidential medical information and keep it separate from regular personnel files and store it in a different, confidential medical file.

2. **Genetic Privacy Concerns (GINA)**

GINA prohibits employers from acquiring or using genetic information in employment decisions. Some wearable technologies, particularly those that analyze DNA or biometric patterns, could inadvertently collect genetic data, placing employers at risk of noncompliance. Moreover, employees must be informed about how their data is being collected and utilized.

Employer Tip:

Employers should confirm that wearable tech does not collect or process genetic data and should avoid using any insights related to family medical history in employment considerations.

3. **Disparate Impact and Bias (Title VII)**

If wearable technology is used in ways that disproportionately impact certain groups—whether by race, color, religion, sex, national origin, gender, or age—it may constitute a Title VII violation. Given that this is such new technology, it is possible that wearables could generate inaccurate data for certain groups of employees, leading to potential discrimination, even if such discrimination is inadvertent. For instance, if an employer uses a biometric scanner to monitor productivity and the algorithm favors one demographic over another, it could lead to claims of disparate impact discrimination.

Moreover, any corresponding adverse employment action employee based on that faulty data could then be unlawful. By way of example, the guidance lays out several hypothetical scenarios where employers could be engaging in unlawful discrimination through their use of wearable technology:

- Using heart rate, fatigue level, and/or temperature information to infer that an employee is pregnant, and then as a result firing the employee or putting her on unpaid leave against her will.
- Relying on data from wearable technology that produces less accurate results for individuals with dark skin to make adverse employment decisions against those workers.
- Firing an employee based on an elevated heart rate when the elevated heart rate results from a heart condition.
- Tracking an employee during their lunch break when the employee is taking their parent to a dialysis center and then inquiring or conducting research about the purpose for the employee's visit to the center, in a way that elicits genetic information, which includes family medical history.
- Analyzing heart rate variability and skin temperature to infer or predict menopause, and then refusing to promote the employee because of sex, age, and/or disability.

In addition, an employer may not selectively use wearables to monitor certain employees based on a protected characteristic or in retaliation for an employee engaging in protected activity. For example, requiring only Hispanic employees to use wearables that collect health information, as the disparate treatment of Hispanic employees based on their national origin could violate EEO nondiscrimination requirements. Similarly, it would also be unlawful to increase surveillance or scrutiny of employees who assert their rights in order to retaliate against them for engaging in protected EEO activity, without similarly monitoring other workers.

Employer Tip:

Employers should audit any and all employment-related decisions arising out of wearable tech programs for potential bias, ensuring that data-driven decisions do not lead to inadvertent discrimination or disproportionate impacts on the population of your workforce and any adverse employment decisions are not made in haste based on data gleaned from wearable technology. They should also ensure transparency in how these devices influence employment decisions.

Additionally, companies should apply their policies uniformly across their workforce (or across divisions, and specific job function, etc.) and be sure not to use the information gathered as a tool for targeting or retaliating against certain employees. Indeed, requiring that a device be worn by only some small subset of your work population that you have singled (even for perceived safety-reasons), such as all pregnant employees or all employees who have complained about various aspects of their job, could be the basis for a claim of unlawful discrimination or retaliation under the National Labor Relations Act or other labor and employment statutes.

Biometric Privacy Laws and Compliance Considerations

In addition to EEOC regulations, employers must be mindful of biometric privacy laws such as the Illinois Biometric Information Privacy Act (BIPA), which imposes strict requirements on businesses collecting, storing, and using biometric data, including the need for informed consent, limited data retention, and strong security measures. Similarly, the Texas Data Privacy and Security Act (TDPSA) includes provisions related to biometric data, requiring businesses to obtain explicit consent before collecting biometric identifiers and to take reasonable measures to protect such data. Non-compliance with these laws and similar regulations in other states can result in significant legal and financial risks.

Key Takeaways for Employers Implementing Wearable Technology

To mitigate risks while leveraging the benefits of wearable tech, employers should adopt the following best practices:

- **Implement Clear Policies:** Define the scope of data collection, usage, and storage to ensure compliance with employment laws.
- **Ensure Voluntary Participation:** Employees should not feel coerced into using wearable technology, especially when it involves personal health data.
- **Maintain Data Privacy and Security:** Employers must ensure that wearable device data is securely stored and protected against breaches.
- **Engage in Employee Communication:** Clearly communicate the purpose, benefits, and risks of wearable technologies to foster trust and prevent misunderstandings.
- **Regular Compliance Audits:** Periodic reviews can help employers identify and rectify potential legal vulnerabilities in their wearable tech programs.

Looking Ahead

The EEOC's guidance signals that while wearable technology holds promise for workplace efficiency, employers must be proactive in addressing the associated legal risks. As the legal landscape around wearable technology

and biometric data privacy continues to evolve, staying informed and consulting with legal professionals will be critical. Employers should approach these innovations not just as tools for efficiency, but as part of a broader commitment to ethical and lawful workplace practices.

We trust this analysis of the new guidance issued by the EEOC helps our clients better understand the employment law related risks associated with wearable technologies and provides useful strategies for how to mitigate those risks. As always, contact the attorneys in CMC's national Labor and Employment Practice Group if you have any questions or would like further guidance on these developments.