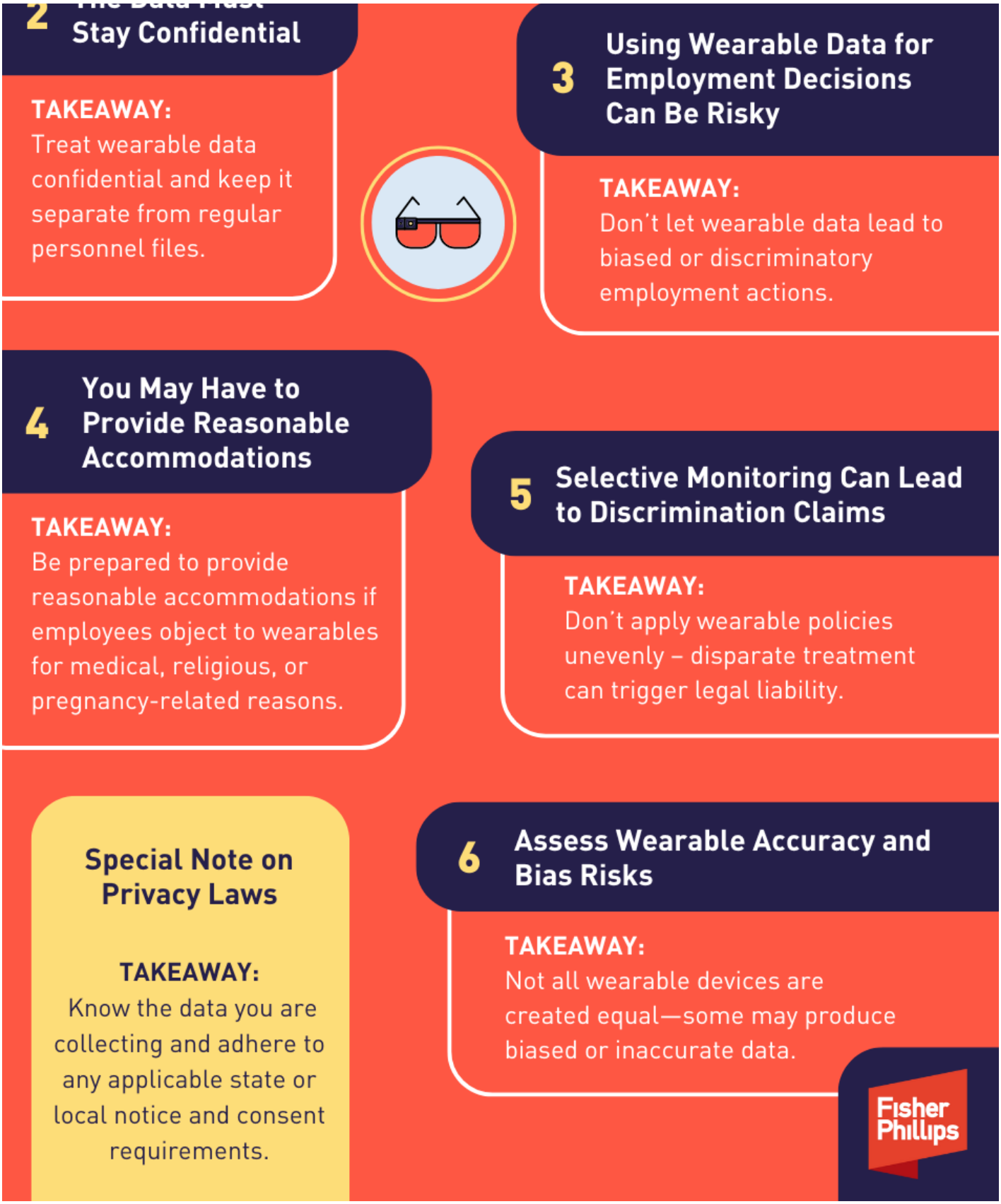
Top 6 Employer Takeaways From New EEOC Wearable Tech Guidance

Insights
1.07.25

Wearable technologies are becoming increasingly common in the workplace, but a new guidance document from the Equal Employment Opportunity Commission (EEOC) has made it clear that employers need to tread carefully. From smart watches and rings to GPS trackers and environmental sensors – and even exoskeletons – wearables collect a wealth of data that could potentially expose employers to legal risks under employment discrimination laws. Here are the top six takeaways for employers from the EEOC's December 19 fact sheet to help you stay compliant and avoid potential pitfalls.



1. Wearables May Involve Disability-Related Inquiries

Takeaway: Don't assume wearable devices are just fitness tools – collecting health-related data can trigger ADA compliance

requirements.

Wearables that gather information about an employee's physical or mental condition, such as heart rate or fatigue levels, may be considered a medical examination or a disability-related inquiry under the Americans with Disabilities Act (ADA). You can only conduct such inquiries if they are job-related and consistent with business necessity or fall within narrow exceptions.

Action Item: Review your wearable device policies to ensure that any health-related data collection complies with ADA rules. Limit the use of wearables for medical data collection unless it's essential to job performance and safety.

2. Medical Data Must Stay Confidential

Takeaway: Treat medical or disability-related data collected from wearable devices as confidential medical information and keep it separate from regular personnel files.

Even if you are allowed to collect such data under the ADA, make sure it is stored in a separate, confidential medical file.

Action Item: Implement secure data storage practices for wearable-generated information. Ensure only authorized personnel have access. Review your employee privacy policies to ensure compliance with ADA confidentiality requirements.

3. Using Wearable Data for Employment Decisions Can Be Risky

Takeaway: Don't let wearable data lead to biased or discriminatory employment actions.

The EEOC guidance notes that using wearable data to make employment decisions – such as firing an employee based on health metrics or fatigue levels – can lead to discrimination claims. This is particularly concerning if the data has different accuracy levels based on characteristics like skin color, gender, or age. For example, an employer using a wearable to monitor employee stress levels might inadvertently discriminate if the device is less accurate for certain racial groups.

Action Item: Ensure that wearable data isn't used as the sole basis for employment decisions. Conduct regular audits to check for potential biases in how wearable data is collected and used.

4. You May Have to Provide Reasonable Accommodations

Takeaway: Be prepared to provide reasonable accommodations if employees object to wearables for medical, religious, or pregnancy-related reasons.

Even if the use of a wearable device is lawful under the ADA, you may still need to make accommodations under federal laws, including Title VII and the Pregnant Workers Fairness Act. This could mean allowing an employee to opt out of wearing a device or offering an alternative.

Action Item: Establish a process for employees to request accommodations related to wearables, and train supervisors to handle such requests appropriately.

5. Selective Monitoring Can Lead to Discrimination Claims

Takeaway: Don't apply wearable policies unevenly – disparate treatment can trigger legal liability.

Employers that selectively require certain employees to wear devices based on protected characteristics, such as national origin or age, may face discrimination claims. Similarly, increasing wearable monitoring on employees who assert their workplace rights could be considered retaliation.

Action Item: Apply wearable policies uniformly across your workforce. Avoid using wearables as a tool for targeting or retaliating against specific employees.

6. Assess Wearable Accuracy and Bias Risks

Takeaway: Not all wearable devices are created equal—some may produce biased or inaccurate data.

The EEOC warns that wearables might generate inaccurate data for certain groups of employees, leading to potential discrimination. Devices that measure biometric data may not account for differences in skin tone, gender, or age, which can skew results.

Action Item: Vet wearable devices before deploying them in the workplace. Check for any known accuracy issues across different demographics and ensure that the devices are validated for diverse populations. Avoid making employment decisions based solely on wearable data.

Special Note on Privacy Laws

Takeaway: Know the data you are collecting and adhere to any applicable state or local notice and consent requirements.

While the EEOC fact sheet focused on the EEO aspects of wearable tech, recognize that collecting wearable data may also trigger notice, consent, and other requirements pursuant to applicable privacy laws. Depending upon the nature of the device and the data collected, the use of a wearable device may trigger the application of biometric information privacy statutes. This includes Illinois' Biometric Information Privacy Act (BIPA), workplace surveillance statutes (such as those in Connecticut and New York), or location tracking legislation that limits the use of mobile tracking devices. In addition, knowing where your data is stored and how it may potentially be used – including by third parties that touch the data collected from wearables – may also implicate additional compliance obligations under various privacy laws.

Action Item: Identify the location of employees who will be asked to use wearable devices, as well as the data to be collected by such devices, and obtain advice regarding applicable notice or consent requirements prior to the implementation of any wearable device program. Review agreements with third parties that have access to the data and ensure you have appropriate contractual and security safeguards in place.

Conclusion

For more information, contact your Fisher Phillips attorney or the authors of this Insight. Make sure to sign up for Fisher Phillips Insights to stay up to speed on the latest developments.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner

Partner
610.230.2132
Email

Anne Yarovoy Khan
Of Counsel
949.798.2162
Email

Service Focus

Employment Discrimination and Harassment

Employee Leaves and Accommodations

Counseling and Advice

Privacy and Cyber