Insights, News & Events

WEARABLES ARE CHANGING SPORTS EMPLOYMENT: WHAT TEAMS AND SCHOOLS SHOULD KNOW ABOUT ATHLETE BIOMETRIC DATA

Insights
Aug 3, 2026

Wearables Are Changing Sports Employment: What Teams And Schools Should Know About Athlete Biometric Data

As teams, schools, and other sports employers collect increasingly detailed biometric data through wearable technologies, questions about who owns that data, how it can be used, and what legal protections apply are becoming just as important as the technology itself. Recent NCAA guidance on the responsible use of performance technologies reflects this shift, emphasizing that institutions should think beyond athletic performance and develop clear governance for athlete data. This Insight explains why wearable technology is a sports employment issue, the evolving legal landscape, and practical considerations for sports employers that collect, use, or share athlete biometric data.

Wearable Technology Has Become Standard Practice, and the NCAA Is Responding

Professional teams, colleges, and even many high schools now routinely use wearable technologies like Whoop, Oura, and Garmin to track heart rate, sleep, movement patterns, location, and more. The data is valuable for informing injury prevention, workload management, rehabilitation, player development, and return-to-play decisions.

But, this also produces enormous amounts of sensitive, personal data, creating questions about the appropriate and

Related People



Adam F. Sloustcher

Regional Managing Partner, Co-Chair of Sports Industry Team

214.220.8304

Service Focus

Privacy and Cyber

Workplace Safety

Industry Focus

Sports

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

legal use of athlete data, especially as it becomes the industry standard for team management, contract negotiations, and more.

The NCAA Committee on Competitive Safeguards and Medical Aspects of Sports recently urged member institutions to think more intentionally about topics like informed consent, written governance plans, and data ownership, security, and retention. The NCAA's performance technology report and recommendations don't create new legal obligations, but they underscore the fact that athlete biometric data is increasingly being scrutinized as a governance and privacy issue.

What Does This Mean for the Sports Industry?

Athlete biometric data has become a valuable asset, but it may also carry significant legal and reputational risks without appropriate safeguards. The legal landscape governing this information is also extremely complex and fragmented. Unlike more traditional employment records, there is no single federal law that comprehensively regulates athlete biometric data. Instead, employers may need to navigate overlapping federal, state, contractual, and institutional requirements depending on the nature of the organization, the data being collected, and how that information is ultimately used. As wearable technologies continue to evolve, sports employers should expect greater scrutiny from regulators, athletes, and the public regarding their data governance practices.

Practical Considerations

Because no single legal framework comprehensively governs the collection, use, or ownership of athlete biometric data, sports employers should evaluate their practices through multiple legal lenses while also considering broader governance and privacy issues.

Employers should consider overlapping obligations under:

- state biometric and consumer privacy laws;
- Family Educational Rights and Privacy Act (FERPA) (student-athlete records);
- HIPAA, where applicable;

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

- Americans with Disabilities Act (ADA) and the Genetic Information Nondiscrimination Act (GINA), where employment decisions are involved; and
- applicable collective bargaining agreements.

Sports businesses should also consider the following practices to get ahead of potential legal issues that arise from the collection and use of athlete biometric data:

1. Develop clear governance policies that address data collection, ownership, retention, security, and access rather than relying on informal practices. Employers should also create rules that address how sensitive data may later influence decisions such as scholarships, compensation, contracts, NIL, roster decisions, and AI development.

2. Be transparent about data collection. Clearly explain what information is being collected, why it is being collected, who will have access to it, how long it will be retained, and whether it may be shared with third parties. Providing this information in plain language can help athletes make informed decisions and demonstrate an employer's commitment to responsible data stewardship.

3. Review vendor relationships. Many wearable technologies rely on third-party vendors to collect, process, analyze, or store athlete data. Employers should understand who ultimately controls that information and carefully review vendor agreements to determine whether data may be used for purposes beyond the employer's intended use, such as product development or AI model training. Contracts should also address data security, confidentiality, breach notification, and procedures for returning or deleting data when the relationship ends.

4. Monitor legal developments. The legal framework surrounding athlete biometric data continues to evolve. Employers should stay informed about developments in state privacy laws, future NCAA guidance, employment law, consumer privacy regulation, and professional sports collective bargaining agreements. Periodically reviewing data governance practices can help employers adapt as legal requirements and industry expectations continue to develop.

Conclusion

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

We will continue to monitor developments and provide updates as warranted. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on our Sports Industry Team or Privacy and Cyber Team.

This Insight was co-authored by Law Clerk Sydney Graves.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.