International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

Cybersecurity and Data Privacy Challenges in Wearable Technologies and Digital Sports Analytics: A Narrative Review

Navdeep Kaur[1], Inderpreet Singh Hirkiar[2]

[1]*Assistant Professor, School of Physical Education, GNA University, Phagwara, Punjab, India*
[2]*Student, School of Engineering, Design, and Automation, GNA University, Phagwara, Punjab, India*

***Abstract*-- The rapid integration of wearable technologies, mobile applications, cloud computing, artificial intelligence (AI), and digital analytics has transformed physical education and sports. Smartwatches, fitness trackers, global positioning system (GPS) devices, inertial measurement units, heart-rate monitors, smart garments, and other sensor-based systems are increasingly used to monitor physical activity, physiological responses, training load, movement patterns, recovery, and sports performance. These technologies provide important opportunities for individualized training, injury prevention, performance analysis, and physical activity promotion. However, the increasing collection and exchange of athlete and student data have also created substantial cybersecurity and data privacy challenges.**

Wearable and digital sports technologies can collect highly sensitive information, including physiological, biometric, behavioural, performance, and location-related data. Such information may be exposed through insecure communication, weak authentication, software vulnerabilities, cloud misconfiguration, unauthorized access, ransomware, third-party data sharing, reidentification, and artificial intelligence-enabled inference. The consequences of compromised sports data may extend beyond conventional privacy concerns because athlete information can influence team selection, competitive strategy, professional contracts, and organizational decision-making.

This narrative review examines cybersecurity and data privacy challenges associated with wearable technologies and digital sports analytics in physical education and sports. It discusses the growing use of digital technologies, major categories of data collected, cybersecurity threats, privacy and reidentification risks, athlete surveillance, informed consent, data ownership, artificial intelligence, ethical and legal concerns, and practical cybersecurity strategies. The review further identifies implications for physical education teachers, coaches, sports scientists, students, athletes, sports organizations, and computer science researchers.

The review concludes that cybersecurity and privacy protection should be considered fundamental components of sports technology adoption. Future digital sports ecosystems should adopt privacy-by-design, security-by-design, data minimization, strong authentication, encryption, role-based access control, cybersecurity awareness programmes, transparent governance, and athlete-centred data policies.

Interdisciplinary collaboration between physical education and sports professionals, computer scientists, cybersecurity specialists, policymakers, and technology developers is essential for ensuring that technological innovation enhances performance and participation without compromising privacy, autonomy, safety, or trust.

***Keywords*--Artificial intelligence; athlete data; cybersecurity; data privacy; digital sports analytics; physical education; sports technology; wearable technology.**

I. INTRODUCTION

Digital technology has become an increasingly important component of physical education, exercise science, sports training, and athletic performance. The traditional methods of observing physical activity and evaluating sports performance are now complemented by wearable devices, mobile applications, cloud-based platforms, artificial intelligence, computer vision, and advanced data analytics. These technologies allow the continuous collection and analysis of information concerning movement, exercise behaviour, physiological responses, training load, recovery, and athletic performance.

Wearable activity trackers are among the most visible examples of this transformation. Such devices can measure steps, distance, heart rate, sleep, movement patterns, and other health- and fitness-related indicators. Their use has expanded beyond personal fitness into organized sport, rehabilitation, sports medicine, physical education, and scientific research. Shin et al. (2019) identified the growing importance of wearable activity trackers and highlighted research trends related to technology, data, adoption, health, behaviour change, and privacy.

In sports, wearable sensor technologies have become increasingly sophisticated. Accelerometers, gyroscopes, inertial measurement units, force sensors, GPS trackers, and physiological monitoring systems can provide detailed information about athlete movement and physical responses. Recent reviews have demonstrated that wearable technologies are being applied across athletic training, rehabilitation, and sports research for monitoring gait, joint motion, pressure, velocity, heart rate, sleep, biomechanics, and sport-specific performance (Olsen et al., 2025).

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

The growth of these technologies has created significant opportunities. Coaches can monitor training loads, sports scientists can analyse movement patterns, and physical education professionals can use digital systems to encourage activity and provide feedback. Artificial intelligence can further assist in processing large volumes of sensor data and identifying patterns that may not be easily detected through traditional observation.

However, technological progress also creates new risks. Wearable devices collect information that can be highly personal and sensitive. Physiological information, movement patterns, behavioural data, and location records may reveal details about an individual's lifestyle, health, identity, or daily routine. A major survey by Niksirat et al. (2024) reviewed 236 studies and concluded that wearable activity trackers raise substantial utility, privacy, and security concerns. The authors noted that wearable data may potentially be used to infer private information and that these devices may be vulnerable to different forms of attack.

The sports environment creates additional complexity because athlete data may possess competitive and commercial value. Information concerning training, physiological condition, injury status, or performance may influence strategic decisions and professional opportunities. Consequently, unauthorized access to athlete information may affect not only privacy but also competitive integrity and professional welfare.

The increasing adoption of cloud computing and connected devices also expands the potential attack surface. Data may travel from a wearable sensor to a smartphone, then to a mobile application, cloud server, analytics platform, or organizational database. Every stage of this information ecosystem may contain vulnerabilities.

The privacy implications of wearable data are particularly important because deidentification alone may not guarantee anonymity. A systematic review by Naeini et al. (2023) found that wearable-device data could often be used for identification or reidentification, with reported identification rates frequently ranging from 86% to 100%. These findings demonstrate that sensor data previously considered anonymous may still create substantial privacy risks.

The use of digital technologies also raises ethical concerns concerning surveillance and autonomy. Athletes may feel pressure to participate in monitoring programmes because coaches, teams, universities, or sports organizations control important opportunities. Students in physical education settings may similarly experience unequal power relationships. Therefore, informed consent and voluntary participation require careful consideration.

Artificial intelligence introduces further opportunities and challenges. AI can support anomaly detection, cybersecurity monitoring, performance analysis, injury-risk research, and individualized training. At the same time, AI systems may introduce algorithmic bias, privacy leakage, data poisoning, adversarial attacks, and automated decision-making concerns.

The intersection of physical education, sports technology, and cybersecurity is therefore an emerging interdisciplinary research area. Physical education professionals require greater awareness of data security, while computer science and cybersecurity researchers need to understand the practical and ethical context in which sports data are generated and used.

This narrative review examines cybersecurity and data privacy challenges associated with wearable technologies and digital sports analytics. It aims to synthesize the major risks, ethical concerns, and practical strategies relevant to the development of safer and more responsible digital sports ecosystems.

II. Objectives Of The Review

The objectives of this narrative review are:

1. To examine the increasing use of wearable technologies and digital analytics in physical education and sports.
2. To identify the major categories of physiological, biometric, behavioural, performance, and location data collected through sports technologies.
3. To examine major cybersecurity threats affecting wearable devices and digital sports analytics systems.
4. To analyse data privacy and reidentification risks associated with wearable technologies.
5. To discuss athlete surveillance, informed consent, autonomy, and data ownership.
6. To examine the role of artificial intelligence in sports cybersecurity.
7. To identify ethical and legal challenges associated with athlete and student data.
8. To provide practical cybersecurity recommendations for sports and educational organizations.
9. To identify research gaps and future directions for interdisciplinary research involving physical education, sports science, computer science, and cybersecurity.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

III. Narrative Review Methodology

This article was designed as a narrative review. A narrative review is appropriate for examining a broad, interdisciplinary topic that combines physical education, sports technology, wearable computing, data privacy, cybersecurity, and artificial intelligence.

The literature relevant to this review includes research on wearable activity trackers, wearable sensors in sports, sports medicine technologies, privacy and security of connected devices, data deidentification, artificial intelligence, and athlete data governance.

Priority was given to peer-reviewed journal articles, systematic reviews, narrative reviews, and influential scholarly publications addressing the following broad concepts:

- Wearable technology
- Sports technology
- Physical activity monitoring
- Athlete monitoring
- Sports analytics
- Cybersecurity
- Data privacy
- Biometric data
- Reidentification
- Artificial intelligence
- Internet of Things

The purpose of the review was interpretative and integrative rather than quantitative. Therefore, no primary data were collected from athletes, students, teachers, coaches, or sports organizations.

This paper does not claim to be a PRISMA-based systematic review because a systematic review requires a predefined and fully documented search strategy, screening process, inclusion criteria, and study-selection procedure. No PRISMA flow diagram or numerical study-selection results have been fabricated for this manuscript.

The literature was synthesized thematically according to major issues relevant to the topic, including technology use, data types, cybersecurity threats, privacy concerns, ethics, governance, artificial intelligence, and future directions.

IV. Digital Transformation In Physical Education And Sports

The digital transformation of physical education and sports has accelerated due to improvements in sensor technologies, mobile computing, wireless communication, cloud infrastructure, and artificial intelligence.

Physical education is increasingly influenced by mobile applications and digital platforms that provide opportunities to monitor activity, deliver feedback, encourage goal setting, and support student engagement. Fitness trackers and smartwatches can allow individuals to monitor steps, physical activity, heart rate, and sleep.

Sports organizations use increasingly sophisticated systems. Elite and recreational athletes may be monitored using GPS devices, accelerometers, gyroscopes, inertial measurement units, and physiological sensors.

Aroganam et al. (2019) reviewed wearable technology sensors used in consumer sport applications and demonstrated the broad role of sensors in collecting sport-related information. Similarly, flexible wearable sensors have expanded opportunities to capture both kinematic and physiological information in sports settings.

Digital transformation provides several advantages:

- Continuous data collection
- Individualized training
- Real-time feedback
- Improved performance analysis
- Enhanced physical activity monitoring
- Potential injury prevention
- Improved rehabilitation monitoring

Despite these benefits, increased digitalization also creates increased cybersecurity responsibilities.

Technology adoption should therefore be accompanied by appropriate security and privacy planning.

V. Wearable Technologies Used In Physical Education And Sports

Wearable technology refers to electronic devices that can be worn on the body and are capable of collecting, processing, or transmitting information.

Common examples include:

- Smartwatches
- Fitness trackers
- Heart-rate monitors
- GPS tracking devices
- Accelerometers
- Gyroscopes
- Inertial measurement units
- Smart garments
- Smart footwear

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

- Electromyography devices
- Sleep monitoring systems

Different sensors collect different forms of information.

Accelerometers can measure movement and acceleration. Gyroscopes can provide information about orientation and angular movement. GPS systems can record location, speed, and distance. Physiological sensors may record heart rate and other indicators.

Olsen et al. (2025) reported that wearable sensor devices used in sports medicine include pedometers, accelerometers, encoders, force sensors, GPS trackers, and inertial measurement units. Their applications include athletic training, rehabilitation, and research.

Wearable technologies therefore have substantial value for physical education and sports. However, the same characteristics that make them useful also create risks.

Continuous monitoring means continuous data generation. Wireless communication means data transmission. Cloud integration means data storage outside the physical device. Together, these factors create a complex security environment.

VI. Types Of Data Collected Through Sports Technologies

Digital sports technologies can collect multiple categories of information.

6.1 Physiological Data

Physiological data may include:

- Heart rate
- Heart-rate variability
- Respiratory information
- Skin temperature
- Oxygen-related indicators
- Sleep-related data
- Recovery indicators

Such information may assist training decisions but can also reveal sensitive characteristics.

6.2 Biometric Data

Biometric information may relate to unique or potentially identifiable characteristics.

Examples may include:

- Physiological signals
- Gait characteristics
- Movement patterns
- Facial information
- Behavioural signatures

Biometric information requires enhanced protection because it may be difficult or impossible to change after exposure.

6.3 Performance Data

Performance-related information may include:

- Speed
- Distance
- Acceleration
- Deceleration
- Training load
- Technical performance
- Tactical information
- Competition statistics

Performance information may have commercial and competitive value.

6.4 Location Data

GPS-enabled devices can collect information about:

- Training locations
- Running routes
- Travel patterns
- Movement behaviour

Unauthorized disclosure of location information can create privacy and personal safety risks.

6.5 Behavioural Data

Digital platforms may collect:

- Exercise frequency
- Activity patterns
- Sleep habits
- Device usage
- Training preferences

When multiple categories of information are combined, organizations may create highly detailed profiles of athletes and users.

VII. The Wearable Technology Data Ecosystem

Understanding cybersecurity requires understanding the complete data ecosystem.

A wearable device rarely operates alone.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

A typical data pathway may involve:

Wearable Sensor → Wireless Connection → Smartphone → Mobile Application → Cloud Server → Analytics Platform → Sports Organization

At each stage, data may be vulnerable to security failures.

Device-Level Risks

Potential vulnerabilities include:

- Weak authentication
- Outdated firmware
- Physical theft
- Insecure storage

Communication Risks

Potential vulnerabilities include:

- Unencrypted wireless communication
- Bluetooth attacks
- Interception
- Spoofing

Application Risks

Potential vulnerabilities include:

- Weak passwords
- Poor authentication
- Software vulnerabilities
- Excessive permissions

Cloud Risks

Potential vulnerabilities include:

- Misconfigured storage
- Unauthorized access
- Third-party vulnerabilities
- Poor access management

The cybersecurity of sports technologies must therefore be evaluated across the complete ecosystem rather than focusing only on the wearable device.

VIII. Major Cybersecurity Threats In Wearable Sports Technologies

8.1 Unauthorized Access

Unauthorized access occurs when a person obtains information or enters a system without permission.

Weak passwords and poor authentication can increase the likelihood of unauthorized access.

Sports organizations may hold sensitive information concerning athletes, students, employees, and organizational strategy.

Strong authentication is therefore essential.

8.2 Data Breaches

A data breach occurs when confidential information is exposed, accessed, or disclosed without authorization.

In sports, a breach could expose:

- Athlete personal information
- Physiological data
- Training records
- Performance analytics
- Injury-related information
- Location information

The consequences may affect privacy, athlete welfare, professional opportunities, and competitive integrity.

8.3 Wireless Communication Attacks

Wearable devices frequently depend on:

- Bluetooth
- Wi-Fi
- Mobile networks

Weak security mechanisms can create opportunities for attackers.

Potential risks include:

- Interception
- Spoofing
- Unauthorized pairing
- Man-in-the-middle attacks

Encryption and secure communication protocols are important protective measures.

8.4 Malware and Ransomware

Sports organizations depend on digital systems for:

- Athlete management
- Communication
- Competition administration
- Financial operations
- Ticketing
- Performance analysis

Ransomware can disrupt these operations by encrypting organizational information and restricting access.

Organizations should therefore maintain secure backups and incident response plans.

8.5 Phishing and Social Engineering

Cybersecurity incidents are not always caused by technical vulnerabilities.

Human error can create significant risks.

Attackers may attempt to deceive:

- Coaches
- Athletes
- Administrators
- Teachers
- Sports scientists

Cybersecurity education is therefore essential.

8.6 Cloud Security Risks

Cloud computing provides:

- Scalability
- Accessibility
- Data sharing

However, risks may occur when:

- Access permissions are excessive.
- Storage is incorrectly configured.
- Encryption is inadequate.
- Third-party providers have weak security.

Sports organizations must understand where their information is stored and who can access it.

IX. Data Privacy Challenges In Athlete Monitoring

Data privacy refers to the appropriate collection, use, sharing, storage, and protection of personal information.

Athlete monitoring presents distinctive privacy concerns.

The relationship between an athlete and a sports organization may involve unequal power.

A player may believe that refusing monitoring could negatively affect:

- Team selection
- Playing opportunities
- Professional development
- Relationships with coaching staff

Therefore, consent requires careful consideration.

9.1 Informed Consent

Individuals should understand:

- What data are collected.
- Why data are collected.
- How data will be analysed.
- Who will access the information.
- How long data will be retained.
- Whether data will be shared.

Consent should be understandable and meaningful.

9.2 Data Minimization

Organizations should collect only information necessary for clearly defined purposes.

Technology should not be used for unnecessary surveillance simply because data collection is technically possible.

9.3 Secondary Data Use

Information collected for one purpose may later be used for another.

For example, performance monitoring information might later influence:

- Team selection
- Contract decisions
- Research
- Commercial activities

Secondary data use should be transparent and appropriately governed.

X. Reidentification Risks And The Limitations Of Deidentification

Removing names from a dataset does not automatically guarantee anonymity.

Naeini et al. (2023) systematically examined whether deidentification of wearable data provides adequate privacy protection.

The review identified substantial reidentification concerns.

The findings demonstrate that sensor information may contain patterns capable of identifying individuals.

For example:

- Gait patterns may be distinctive.
- Physiological signals may contain identifying characteristics.
- Movement patterns may be unique.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

The study found that identification rates reported in the literature were frequently between 86% and 100%.

This has important implications for physical education and sports research.

Researchers and organizations should not assume that removing names or identification numbers eliminates privacy risks.

Additional privacy-preserving approaches may be required.

XI. Athlete Surveillance And Autonomy

Wearable technology can create continuous surveillance.

Athletes may be monitored during:

- Training
- Competition
- Recovery
- Travel
- Daily activity

Monitoring may provide useful information, but excessive surveillance can affect autonomy.

An athlete may feel that every activity is being evaluated.

The benefits of monitoring must therefore be balanced against:

- Privacy
- Autonomy
- Dignity
- Psychological well-being

Digital surveillance should have clearly defined boundaries.

XII. Data Ownership In Sports

An important question is:

Who owns athlete data?

Possible stakeholders include:

- Athletes
- Sports organizations
- Universities
- Technology companies
- Sports governing bodies
- Researchers

There is no universally simple answer.

However, governance policies should clearly explain:

- Who controls data.
- Who can access data.
- How data may be shared.
- What happens when an athlete leaves an organization.

Athlete-centred data governance is an important direction for future research.

XIII. Digital Sports Analytics And Competitive Security

Sports analytics platforms can contain strategically important information.

Data may relate to:

- Team performance
- Tactical strategies
- Training plans
- Athlete readiness
- Competition analysis

Unauthorized access may create competitive disadvantages.

Therefore, sports analytics should be protected using:

- Encryption
- Authentication
- Role-based access
- Audit logs
- Secure backups

Cybersecurity should be integrated into the design and operation of sports analytics systems.

XIV. Mobile Applications And Fitness Data

Mobile applications often connect wearable devices to users and organizations.

However, users may not always understand:

- Which data are collected.
- How data are stored.
- Whether data are shared with third parties.
- How long data are retained.

Doherty et al. (2025) examined privacy policies among leading wearable technology manufacturers and identified continuing concerns related to transparency and vulnerability disclosure.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

This finding demonstrates the importance of clear and understandable privacy communication.

Technology providers should adopt transparent policies.

XV. Artificial Intelligence In Sports Technology

Artificial intelligence is increasingly used in:

- Performance analysis
- Movement recognition
- Training recommendations
- Injury-risk research
- Sports analytics

Machine learning can analyse large quantities of sensor data.

Deep learning is increasingly used for sensor-based activity recognition and sports performance monitoring.

Recent research has highlighted the growing use of multimodal sensing approaches that combine wearable sensors, vision-based technologies, and other sources of information.

However, AI systems also create cybersecurity and privacy concerns.

XVI. Artificial Intelligence And Cybersecurity

16.1 AI for Cybersecurity

Artificial intelligence may help organizations:

- Detect unusual activity.
- Identify anomalies.
- Detect potential intrusions.
- Analyse cybersecurity events.

Machine learning may support faster analysis of large datasets.

16.2 AI-Related Risks

AI systems can also introduce risks.

These include:

- Algorithmic bias
- Data poisoning
- Model manipulation
- Adversarial attacks
- Privacy leakage
- Unauthorized inference

AI systems should therefore be evaluated from both performance and security perspectives.

16.3 Explainable Artificial Intelligence

Explainability is important when AI influences athlete-related decisions.

Professionals should understand:

- How recommendations are generated.
- Which data are used.
- What limitations exist.

AI should support professional decision-making rather than completely replace human judgement.

XVII. Ethical Challenges

Technology adoption should be guided by ethical principles.

17.1 Autonomy

Individuals should have meaningful control over their personal information.

17.2 Transparency

Organizations should explain how data are collected and used.

17.3 Fairness

Technology should not unfairly disadvantage individuals.

17.4 Accountability

Organizations should accept responsibility for protecting data.

17.5 Privacy

Personal information should be protected from unnecessary collection and unauthorized access.

17.6 Equity

Digital technologies should not increase inequality in sports participation.

XVIII. Legal And Regulatory Considerations

Data protection requirements differ across countries.

However, important principles generally include:

- Lawful collection
- Purpose limitation
- Data minimization
- Transparency
- Security
- Accountability

Biometric and health-related information may require additional protection.

Sports organizations operating internationally should understand the relevant legal requirements affecting athlete information.

XIX. Cybersecurity Implications For Physical Education

Physical education institutions increasingly use digital technologies.

However, educational settings require special attention because institutions have responsibilities toward students.

Before implementing wearable monitoring systems, institutions should consider:

1. Why the technology is necessary.
2. Whether less intrusive alternatives exist.
3. Which data are collected.
4. How data are stored.
5. Who can access the information.
6. How long data are retained.

Physical education teachers should receive basic training concerning:

- Data privacy
- Cybersecurity awareness
- Responsible technology use

XX. Cybersecurity Implications For Coaches And Sports Scientists

Coaches and sports scientists increasingly work with digital information.

However, access to data creates responsibility.

Professionals should understand:

- Data sensitivity
- Secure storage
- Appropriate sharing
- Access limitations

Athlete information should not be shared casually through unsecured applications.

Sports organizations should establish clear procedures for data management.

XXI. Implications For Computer Science And Cybersecurity Students

The topic provides an important opportunity for interdisciplinary research.

Computer science students can contribute to:

- Secure wearable communication
- Privacy-preserving analytics
- Federated learning
- Secure cloud systems
- Anomaly detection
- Artificial intelligence security
- Data encryption

Collaboration with physical education professionals is essential because cybersecurity systems must address real-world sports requirements.

XXII. Privacy-By-Design

Privacy-by-design means integrating privacy protections into technology development from the beginning.

Important principles include:

- Data minimization
- User control
- Transparent communication
- Secure defaults

Privacy should not be added only after a problem occurs.

XXIII. Security-By-Design

Security-by-design means incorporating cybersecurity into every stage of technology development.

Important measures include:

- Secure software development
- Encryption
- Strong authentication
- Regular testing
- Vulnerability management

Security should be considered before deployment.

XXIV. Practical Cybersecurity Framework For Sports Organizations

A practical framework can be organized into six stages.

Stage 1: Identify

Identify:

- Sensitive data
- Important systems
- Potential threats

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

- Organizational vulnerabilities

Stage 2: Protect

Implement:

- Strong passwords
- Multi-factor authentication
- Encryption
- Access controls

Stage 3: Detect

Monitor:

- Unusual activity
- Unauthorized access
- Suspicious network behaviour

Stage 4: Respond

Develop an incident response plan.

Stage 5: Recover

Maintain secure backups and recovery procedures.

Stage 6: Educate

Provide cybersecurity awareness programmes.

Table 1. Major Digital Technologies Used in Physical Education and Sports

Technology	Major Applications	Types of Data	Major Privacy/Security Risks
Smartwatch	Activity and health monitoring	Heart rate, activity, sleep	Unauthorized access
GPS tracker	Movement and workload monitoring	Location, speed, distance	Location exposure
Accelerometer	Movement analysis	Acceleration and activity	Data interception
IMU	Biomechanical assessment	Motion and orientation	Reidentification
Mobile application	Data visualization	Personal and behavioural data	Third-party sharing
Cloud platform	Data storage and analytics	Multiple athlete datasets	Cloud misconfiguration
AI analytics	Performance prediction	Multimodal data	Bias and privacy leakage

Table 2. Major Cybersecurity Threats in Sports Technologies

Threat	Description	Possible Consequence
Unauthorized access	Access without permission	Athlete data exposure
Data breach	Unauthorized disclosure	Privacy and reputational harm
Ransomware	Data/system encryption	Operational disruption
Phishing	Deceptive communication	Credential theft
Wireless attack	Interception of communication	Data theft
Cloud vulnerability	Weak cloud configuration	Large-scale exposure
AI attack	Manipulation of AI systems	Incorrect decisions

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

Table 3. Recommended Data Protection Measures

Area	**Recommended Measure**
Authentication	Multi-factor authentication
Data transmission	Encryption
Data storage	Secure encrypted storage
Access	Role-based access control
Privacy	Data minimization
Human security	Cybersecurity training
Incident management	Response and recovery plan
Governance	Clear data policies
Technology design	Privacy-by-design

XXV. Major Research Gaps

Several important research gaps remain.

First, cybersecurity research specifically focused on sports remains limited.

Second, more research is needed on the security of athlete monitoring systems.

Third, the long-term consequences of biometric surveillance require investigation.

Fourth, athlete and student perspectives should receive greater attention.

Fifth, cybersecurity awareness among coaches and physical education teachers requires further study.

Sixth, more research is needed on practical privacy-preserving technologies.

Seventh, AI security in sports requires further investigation.

XXVI. Future Directions

Future research should prioritize:

1. Athlete-Centred Data Governance

Athletes should have greater participation in decisions concerning their data.

2. Privacy-Preserving Analytics

Technologies should reduce unnecessary exposure of sensitive information.

3. Federated Learning

Federated learning may enable collaborative machine learning while reducing the need to centralize raw information.

4. Explainable AI

Sports AI systems should provide understandable explanations.

5. Cybersecurity Education

Sports professionals require practical cybersecurity training.

6. Interdisciplinary Collaboration

Physical education, sports science, computer science, and cybersecurity researchers should work together.

7. Standardized Guidelines

The sports sector would benefit from clearer cybersecurity guidelines for wearable technology.

XXVII. Strengths Of The Present Review

The review integrates literature from:

- Physical education
- Sports science
- Wearable technology
- Cybersecurity
- Data privacy
- Artificial intelligence

This interdisciplinary approach provides a broader understanding of the topic.

The review also emphasizes practical implications rather than focusing exclusively on technical issues.

XXVIII. Limitations Of The Present Review

This article is a narrative review rather than a systematic review.

Therefore:

- It does not include a PRISMA flow diagram.
- It does not report a formal numerical study-selection process.
- It does not conduct a meta-analysis.

The purpose of the review is to provide an interdisciplinary synthesis of the major challenges and future directions.

Future researchers may conduct a systematic review focusing specifically on cybersecurity incidents, privacy vulnerabilities, or athlete biometric data governance.

XXIX. Conclusion

The rapid adoption of wearable technologies and digital sports analytics has transformed physical education and sports. Smartwatches, fitness trackers, GPS devices, inertial sensors, cloud platforms, and artificial intelligence systems provide significant opportunities for physical activity monitoring, individualized training, performance analysis, rehabilitation, and sports science research.

However, these benefits are accompanied by important cybersecurity and data privacy challenges. Wearable technologies may collect sensitive physiological, biometric, behavioural, performance, and location-related information. This information may be exposed through unauthorized access, insecure communication, cloud vulnerabilities, phishing, ransomware, reidentification, and inappropriate data sharing.

Sports organizations must therefore recognize cybersecurity as an essential component of modern sports technology.

Privacy protection should not be treated as a secondary concern. Athletes and students should understand what information is collected, why it is collected, who can access it, and how it will be used.

The findings of this review suggest that future digital sports ecosystems should adopt privacy-by-design and security-by-design principles. Strong authentication, encryption, access control, data minimization, transparent governance, cybersecurity education, and incident response planning should become standard components of technology implementation.

Artificial intelligence offers significant opportunities for sports and cybersecurity but must be implemented responsibly. Explainability, fairness, privacy protection, and security should be considered throughout the development and deployment of AI systems.

The intersection of physical education and cybersecurity represents an important emerging area of interdisciplinary research. Collaboration between physical education professionals, sports scientists, computer scientists, cybersecurity specialists, technology developers, policymakers, coaches, athletes, and students will be essential.

Ultimately, technology should enhance physical education and sports without compromising privacy, autonomy, security, or trust. The future success of digital sports technologies will depend not only on their ability to collect and analyse information but also on their ability to protect the individuals whose data make these technologies possible.

REFERENCES

[1] Aroganam, G., Manivannan, N., & Harrison, D. (2019). Review on wearable technology sensors used in consumer sport applications. *Sensors, 19*(9), 1983. https://doi.org/10.3390/s19091983

[2] Bull, F. C., Al-Ansari, S. S., Biddle, S., Borodulin, K., Buman, M. P., Cardon, G., Carty, C., Chaput, J.-P., Chastin, S., Chou, R., Dempsey, P. C., DiPietro, L., Ekelund, U., Firth, J., Friedenreich, C. M., Garcia, L., Gichu, M., Jago, R., Katzmarzyk, P. T., ... Willumsen, J. F. (2020). World Health Organization 2020 guidelines on physical activity and sedentary behaviour. *British Journal of Sports Medicine, 54*(24), 1451–1462. https://doi.org/10.1136/bjsports-2020-102955

[3] Dang, L. M., Min, K., Wang, H., Piran, M. J., Lee, C. H., & Moon, H. (2020). Sensor-based and vision-based human activity recognition: A comprehensive survey. *Pattern Recognition, 108*, 107561. https://doi.org/10.1016/j.patcog.2020.107561

[4] Demrozi, F., Pravadelli, G., Bihorac, A., & Rashidi, P. (2020). Human activity recognition using inertial, physiological, and environmental sensors: A comprehensive survey. *IEEE Access, 8*, 210816–210836. https://doi.org/10.1109/ACCESS.2020.3037705

[5] Doherty, C., et al. (2025). Privacy in consumer wearable technologies: A living systematic analysis of data policies across leading manufacturers. *npj Digital Medicine*. https://doi.org/10.1038/s41746-025-01757-1

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

[6] Lara, O. D., & Labrador, M. A. (2013). A survey on human activity recognition using wearable sensors. *IEEE Communications Surveys & Tutorials, 15*(3), 1192–1209. https://doi.org/10.1109/SURV.2012.110112.00192

[7] Naeini, E. K., et al. (2023). Does deidentification of data from wearable devices give us a false sense of security? A systematic review. *The Lancet Digital Health*.

[8] Niksirat, K. S., Velykoivanenko, L., Zufferey, N., Cherubini, M., Huguenin, K., & Humbert, M. (2024). Wearable activity trackers: A survey on utility, privacy, and security. *ACM Computing Surveys, 56*(7), Article 183. https://doi.org/10.1145/3645091

[9] Nweke, H. F., Teh, Y. W., Al-Garadi, M. A., & Alo, U. R. (2018). Deep learning algorithms for human activity recognition using mobile and wearable sensor networks: State of the art and research challenges. *Expert Systems with Applications, 105*, 233–261. https://doi.org/10.1016/j.eswa.2018.03.056

[10] Olsen, R. J., Hasan, S. S., Woo, J. J., Nawabi, D. H., & Ramkumar, P. N. (2025). The fundamentals and applications of wearable sensor devices in sports medicine: A scoping review. *Arthroscopy, 41*(2), 473–492. https://doi.org/10.1016/j.arthro.2024.01.042

[11] Shoaib, M., Bosch, S., Incel, O. D., Scholten, H., & Havinga, P. J. M. (2015). A survey of online activity recognition using mobile phones. *Sensors, 15*(1), 2059–2085. https://doi.org/10.3390/s150102059

[12] Shin, G., Jarrahi, M. H., Fei, Y., Karami, A., Gafinowitz, N., Byun, A., & Lu, X. (2019). Wearable activity trackers, accuracy, adoption, acceptance, and health impact: A systematic literature review. *Journal of Biomedical Informatics, 93*, 103153. https://doi.org/10.1016/j.jbi.2019.103153

[13] Stavropoulos, T. G., Papastergiou, A., Mpaltadoros, L., Nikolopoulos, S., & Kompatsiaris, I. (2020). IoT wearable sensors and devices in elderly care: A literature review. *Sensors, 20*(10), 2826. https://doi.org/10.3390/s20102826

[14] Tao, W., Liu, T., Zheng, R., & Feng, H. (2012). Gait analysis using wearable sensors. *Sensors, 12*(2), 2255–2283. https://doi.org/10.3390/s120202255

[15] Tunca, C., Pehlivan, N., Ak, N., Arnrich, B., Salur, G., & Ersoy, C. (2017). Inertial sensor-based robust gait analysis in non-hospital settings for neurological disorders. *Sensors, 17*(4), 825. https://doi.org/10.3390/s17040825

[16] Wang, J., Chen, Y., Hao, S., Peng, X., & Hu, L. (2019). Deep learning for sensor-based activity recognition: A survey. *Pattern Recognition Letters, 119*, 3–11. https://doi.org/10.1016/j.patrec.2018.02.010

[17] Wang, Y., Cang, S., & Yu, H. (2019). A survey on wearable sensor modality-centred human activity recognition in health care. *Expert Systems with Applications, 137*, 167–190. https://doi.org/10.1016/j.eswa.2019.04.057