International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Impact Factor (2020): 6.733

# Data Privacy and Security in Sports: Challenges and Solutions for Protecting Athlete Information

**Bhanuja MK, Fuad VC**

**Abstract:** ***The way athlete data is gathered, saved, and analysed has been revolutionised by the use of information technology in sports. From performance tracking to injury prevention, athlete data has become a crucial component of sports management. However, there are growing worries regarding data security and privacy in sports due to the increased reliance on digital data. The paper discusses issues and suggestions for protecting athlete information. In addition to providing guidelines for practitioners, policymakers, and educators in tackling the complex issues surrounding data privacy and security in sports, these suggestions promote the ethical and responsible management of athlete data.***

**Keywords:** Data Security, Data Privacy, Athlete data, Sports.

## 1. Introduction

Data collection in sports is not a new concept. It has been a common practise to collect athletes' data, notably heart rate, in order to better understand the body and, ultimately, improve performance. What changes is the sort of information that can be acquired, advancements in technology, the ease with which it is gathered, and the methods for storing and manipulating the data [5]. Data collection is no longer confined to the period when an athlete is really training. Data is gathered and evaluated from a wide range of sources, including wearables (watches, monitors), athlete management platforms, and a variety of other technology advances [6]. Personal data is increasingly being gathered and processed to support activities such as player scouting, fan engagement, and event management, hence data privacy and security are key concerns in the field of sports. Personal data gathered in the sports industry comprises not just basic information such as names and contact information, but also sensitive information [1]. Sensitive information includes Data on player health and medical records, contractual and financial information, analytics, digital media (Photos, videos etc.), fan information, and employee information [8]. Insider Threats are the most typical type of risk for every organisation. Insider Threats are those who have authorised access to sensitive data such as players' personal information, financial data, and team strategy but utilise that access for unauthorised purposes [8]. Current or former workers, contractors, or other trusted individuals with access to sensitive information are examples of insiders. This accounts for more than half of all data breaches.

There have been reports of personal data being collected from athletes without the athletes knowledge or consent that over 850 soccer players from the Premier League, EFL, National League, and Scottish Premiership have collectively accused over 150 corporations of using data on their physical health without a legal basis. [2]. Players are frequently asked to disclose personal data to coaches and team officials, such as medical records and training schedules, however this data is occasionally shared with third - party organisations without the players' knowledge or agreement. Third - party access is a valid be concerned as data is handed on to broadcasters, wagering organisations, commercial entities, and fans [3]. The disclosure of private data about an athlete's injuries may put the athlete at a competitive disadvantage while competing against non - injured opponents. Similarly, if a team's financial details are revealed, the team may lose sponsorships or be fined by the league. Furthermore, the disclosure of personal information about a coach may result in legal consequences for the coach [4].

The Privacy Act of 1988 (Privacy Act) is the legislative tool used to promote and preserve individuals' privacy. However, HIPAA, PCI DSS, GDPR and CCPA are some primary data protection rules that apply to professional sports organisations [8]. GDPR (General Data Protection Regulation) regulation which EU's new data protection regulation deals with protection of an individuals personal information [11]. It is critical that sporting bodies understand their obligations under the Privacy Act [7]. If an athlete or another person files a complaint about a violation, the organisation may face regulatory action and subsequent penalties for the violation.

Major League Baseball in North America banned the commercialization of player biometric data in its most recent collective bargaining agreement with the Players' Association however, the subject is handled differently in different sports [2]. The prevention of data breaches is one of the most important advantages of data privacy in a Sports Management platform. When unauthorised individuals gain access to private information, data breaches can occur. Another advantage of data privacy is that it prevents data loss. Data loss can be disastrous, leading to the loss of critical information of athletes and teams. and data privacy contributes to information secrecy [4]. Sports organisations can ensure the integrity and fairness of the sport, safeguard their organisation from financial losses, and ensure the confidentiality and rights of their fans, employees, and player information by implementing effective security measures, complying with relevant data protection regulations, and investing in emerging technologies [8]. Improving information privacy protection technology is a medicinal and sports technological addition. If anonymization is used during the data collecting stage, it can be very effective in various ways of data restriction, and its applicability is also more extensive [9]. In the future there is chance for hackers to hack the electronic equipments used by the athletes used for monitoring their health data and

acquire their information [10].

This paper discusses about the challenges facing by the sports sector on collecting and preserving the athlete data. The possible problems faced while safeguarding the athlete data and the solutions for protecting the information from data breach. Certain ethical considerations are there to taken care of while trying to collect and safeguard the information. Those considerations are also discussing here and the future discussions are also included.

## 2. Case Studies

There have been several incidents in the real world related to data breaches in sports. Here are some of them.

1) **MLB Biogenesis Scandal:** The Biogenesis of America clinic was accused of selling performance - enhancing chemicals to MLB players in 2013. Anthony Bosch, the clinic's founder, received and kept players' personal and health information, including drug test results and treatment details, which were later leaked, resulting in a violation of players' privacy and harming the MLB's reputation.
2) **RIO Olympic Ticketing Data Leak:** Thousands of classified documents, including participants' personal and medical information, were unintentionally made public on the official Rio 2016 Olympics website during the 2016 Rio Olympics. This incident demonstrated the importance of strong data security methods in protecting sensitive athlete information at large sporting events.
3) **WADA Anti - Doping Agency Data Breach:** The Russian hacking group Fancy Bear accessed WADA's Anti - Doping Administration and Management System (ADAMS) and leaked the confidential healthcare records of a number of popular athletes. The compromise was suspected to be politically inspired as it happened after the Russian team encountered a ban from the 2016 Rio Olympics due to state - sponsored dopin.
4) **NFL Medical Record Leak:** A laptop holding hundreds of NFL players' medical records was taken from the car of a Washington Redskins trainer in 2016. The records contained information such as players' injury histories, treatments, and other sensitive information. The event demonstrated the need of encrypting sensitive data and putting in place rigorous access controls.
5) **Starva Fitness App Data Leak:** Through the global heat map feature of the Strava fitness app, which is popular among athletes for monitoring workouts, mistakenly exposed the locations of US Secret military sites in 2018. The event highlighted the possible privacy hazards of sharing personal fitness data, as well as the importance of organisations properly considering the ramifications of data visualisation tools.
6) **Australian Football League (AFL) Data Leak:** The AFL had a data breach, exposing the personal information of thousands of fans who bought tickets to the 2018 AFL Grand Final. The incident occurred owing to a vulnerability in the AFL's third - party ticketing technology, emphasising the importance of organisations ensuring the security of their supply chain partners.
7) **FIFA Data Breach:** FIFA, the governing organisation of international football, had a data breach in 2018 in which confidential information, including details of doping investigations, athlete medical records, and other sensitive data, was accessed and exposed. This incident sparked worries about athlete data security in international sports organisations.
8) **FC Barcelon Twitter Hack:** A group called OurMine hacked FC Barcelona's official Twitter account twice, once in 2017 and again in 2020. The hackers spread bogus information about player transfers and other news, highlighting the potential reputational harm that can occur from poor account security.
9) **NFL Player Data Breach:** In 2020, the National Football League (NFL) faced a data breach in which a hacker obtained unauthorised access to the NFL's player management system and acquired the sensitive data of NFL players, agents, and team officials, including Social Security numbers and contract details. This event highlighted the necessity of athlete data security in professional sports organisations.

## 3. Challenges in Data Privacy and Security in Sports

The widespread use of data in sports has changed how players, teams, and organisations function. Nowadays, data is gathered, saved, and analysed to improve performance, fan engagement, and business decisions in sports. When it comes to data privacy and security in sports, there are substantial difficulties and worries in addition to the advantages. Some of the key challenges are:

### 1) Data Density:

The huge amount of data produced is one of the main issues with data privacy and security in sports. Sports organisations are gathering enormous volumes of data on players, including their performance measurements and biometric data, using wearable technologies, sensors, and other monitoring equipments. Since this information is frequently sensitive, a breach could result in a number of problems, including fraud and identity theft.

### 2) Consent and Openness:

It can be difficult to get athletes' informed consent for data collection and usage. Athletes may not always have enough control over their own data and may not always be fully aware of how it is being gathered, stored, and used. Athletes may not have the time or expertise to fully comprehend the implications of data sharing in fast - paced sports environments, So it can be challenging to ensure transparency in data collection practises, provide concise and comprehensive information about data usage, and obtain informed consent. Organisations must overcome the problem of balancing the demand for data - driven insights with athletes' rights to privacy and control over their data.

### 3) Equality and Fairness:

Data use in sports might generate concerns about fairness and equality. Some athletes, teams, or organisations may not have equitable access to advanced data collection and analysis techniques, giving them an unfair advantage over others. This has the potential to worsen current imbalances in sports and have an influence on the integrity and fairness of sporting events. It is a critical problem to ensure that data

collection and usage practises are equal and do not perpetuate gaps among athletes or teams.

**4) Ethical Considerations:**
The collection and use of athlete data raises concerns about privacy, consent, and fairness. Ethical standards and guidelines are critical in directing the responsible and ethical use of athlete data in the sports sector. To guarantee that athlete data is used responsibly and ethically, questions such as who owns the data, how long it is stored, how it is used, and how it is shared must be addressed ethically. Organisations must think about the ethical implications of data use and make decisions that prioritise athletes' well - being and rights.

**5) Compliance with Regulations:**
Various data privacy and security standards applies to the sports business, such as the General Data Protection Regulation (GDPR) in the European Union, which requires organisations to ensure the privacy and security of personal data. Compliance with these standards can be difficult, as requirements and significance change among jurisdictions. To avoid legal consequences, organisations must negotiate these requirements, implement comprehensive data protection safeguards, and assure compliance. Organisations face a constant challenge in keeping up with new rules and implementing the appropriate procedures to meet compliance requirements.

**6) Technology Advancement:**
The fast pace of technological improvements in sports creates opportunities as well as concerns for data privacy and security. Emerging technologies such as wearable devices, IoT devices, and cloud computing open up novel possibilities for data collecting, storage, and analysis. These technologies, however, bring with them new hazards, such as greater vulnerability to cyber assaults, data breaches, and data misuse. In the sports sector, keeping up with technology innovations and resolving their implications for data privacy and security is a constant problem. To prevent potential attacks, organisations must implement effective cybersecurity safeguards, frequently upgrade their systems, and conduct risk assessments.

**7) Data Breaches:**
Data breaches are one of the most important issues in sports data privacy and security. High - profile data breaches involving athletes' personal and sensitive information caused increased awareness regarding the vulnerability of athlete data. Cybercriminals frequently target sports organisations in order to obtain valuable data, causing reputational harm, financial losses, and legal obligations. To prevent unauthorised access and data leakage, comprehensive security measures such as firewalls, encryption, authentication processes, and personnel training are required.

**Solutions for Protecting Athlete Information**
Organisations might use a combination of technical, administrative, and physical security methods to secure athlete information from data breaches. Some potential solutions for protecting athlete information are:

**1) Encryption:**
Encrypting athlete data is a standard technical preventative measure used to prevent unauthorised access. Encryption is the process of transforming data into a coded format that can only be deciphered with the correct decryption key, rendering it unreadable and unusable to unauthorised individuals or entities. Using powerful encryption methods, encrypt sensitive athlete data both at rest and in transit. This ensures that even if data is intercepted, without the decryption key, it remains unreadable.

**2) Authentication and Access Control:**
Strong authentication and access control mechanisms are useful in preventing unauthorised access to athlete data. Strong passwords, multi - factor authentication, role - based access controls, and regular audits of user access privileges can all be part of this. Implement role - based access control (RBAC) to ensure that only authorised individuals have access to athlete information. Review and adjust access permissions on a regular basis to ensure they stay appropriate.

**3) Strong Authentication:**
Require strong, unique passwords and also needs to enable multi - factor authentication (MFA) for all users who are accessing the athlete information.

**4) Employee Training and Awareness:**
Educating athletes, coaches, and other stakeholders on best practises for data privacy and security can help raise awareness and promote responsible data handling. This can include data privacy and security training programmes, workshops, and guidelines, as well as regular reminders and updates on the need of securing athlete information. Provide continuing data security best practises training to staff members, including how to recognise and report phishing attempts and other possible threats.

**5) Regular Security Audits and Monitoring:**
Regular security audits and monitoring of systems and networks that handle athlete data can aid in the detection and resolution of any vulnerabilities and breaches. Regular security assessments, penetration testing, and monitoring of system logs for suspicious activity and compliance with data protection regulations can all be part of this.

**6) Secure Data Storage:**
Athlete data should be stored in secure, compliant data centres that have strong physical and digital security measures in place. To protect against unauthorised access and potential attacks, employ firewalls, intrusion detection systems, and other network security measures.

**7) Vendor and Third - Party Management:**
If sports organisations rely on third - party suppliers or partners to manage data, it is critical to ensure that proper data privacy and security procedures are in place with these companies. Due diligence in vendor selection, contractual agreements establishing data privacy and security criteria, and frequent audits of vendor practises are all examples of this.

**8) Compliance with Regulations and Standard:**
Compliance with relevant data privacy and security regulations, such as the European Union's General Data Protection Regulation (GDPR), can provide a framework for safeguarding athlete data. Adhering to industry best practises and standards, such as ISO/IEC 27001 for information security management, can also help guarantee that suitable safeguards to protect athlete information are in place.

**9) Data Backup and Recovery:**
Back up athlete data on a regular basis and have a disaster recovery plan in place to ensure that data can be restored in the event of a breach or system failure.

**10) Have an Incident Response Plan:**
Create and keep a detailed incident response plan in place to guide your organization's response to a data breach, including measures for informing affected individuals and regulatory authorities.

## 4. Ethical Considerations

Ethical considerations for data privacy and security in sports concentrate around the proper collecting, storage, and use of athletes', staff's, and fans' personal and sensitive information. Here are some significant ethical considerations to keep in mind:

1) **Consent from the Athletes:**
Before their data is gathered, athletes should be told about how their data will be collected, used, and shared, and they should provide informed consent. This includes being open about the reason for data collection, the categories of data gathered, and who will have access to the data. Athletes should be able to revoke their consent at any time.
2) **Collecting Minimum Data:** Collecting only the data required for the intended purpose and minimising data collection is a significant ethical consideration. Organisations should avoid gathering superfluous data that may violate athletes' privacy. This decreases the possibility of unauthorised access to or misuse of personal information.
3) **Transparency and Accountability:** Organisations must be transparent about their data privacy and security practises, and they must hold themselves accountable for their actions. This includes clear and accessible privacy rules, data management protocols, and ways for athletes to exercise their rights, such as viewing their data, fixing errors, and filing complaints.
4) **Data integrity and accuracy:** It is critical to ensure the accuracy and integrity of athlete data. Organisations should take steps to ensure that the information gathered is accurate, up to date, and complete. Athletes have the right to have any mistakes in their data corrected.
5) **Limiting the purpose:** Use personal data only for the reason for which it was gathered, and avoid repurposing it for unrelated purposes without additional consent.
6) **Data Security:** It is an ethical obligation to protect athlete data against unauthorised access, breaches, and theft. To protect athlete data and prevent data breaches, organisations should use strong security measures like as encryption, access controls, and frequent security audits.
7) **Retention of Data and Disposal:** Personal data should be kept only for as long as necessary to serve the original purpose, and then securely disposed of. Organisations need to establish policies for this.
8) **Fairness and Non - discrimination:** Make certain that data collection and processing practises do not unfairly target or discriminate against specific individuals or groups, and that data - driven decisions are fair and unbiased.
9) **International Policy Considerations:** When collecting and handling athlete data across borders, organisations should be aware of international data privacy rules and regulations, such as GDPR, and ensure compliance.

## 5. Recommendations and Future Research

Privacy should be considered when developing sports - related technologies and systems. Conducting privacy impact assessments, minimizing data collection, implementing data anonymization techniques, and incorporating privacy - enhancing technologies to protect athlete information by default are all part of this. To improve data privacy and security, organisations should consider using sophisticated security technologies such as blockchain, artificial intelligence, and machine learning. These technologies can aid in the detection and prevention of cyber assaults, the secure storage and transmission of data, and the enhancement of access control. To prevent data breaches and unauthorised access to athlete information, sports organisations should continue to invest in comprehensive data protection methods such as encryption, access controls, and intrusion detection systems. Regular security audits and risk assessments should be performed to identify vulnerabilities and potential risks to data privacy and security. Regular monitoring and auditing of data privacy and security practices should be implemented to ensure compliance with relevant laws and regulations, such as GDPR, and other industry standards. Non - compliance should be met with appropriate consequences to deter unethical data practices. And also this will enable organisations to address security weaknesses proactively and reduce the risk of data breaches.

To address data privacy and security concerns in sports, collaboration among sports organisations, players, data scientists, technology providers, and policymakers is critical. Stakeholders should collaborate to produce industry - wide standards, guidelines, and best practises for athlete data protection. Athletes, employees, and supporters should receive frequent training and instruction on data privacy and security best practises from sports organisations. This will contribute to a greater understanding of the dangers and obligations connected with handling personal and sensitive information. Sports organisations must encourage transparency, accountability, and ethical data practices in order to establish a culture of privacy and security. This will aid in the development of trust among stakeholders and indicate a commitment to appropriate data handling. Researchers should do research on emerging challenges and solutions in sports data privacy and security. This will aid in the identification of new threats and opportunities for strengthening data security in the sports business.

## 6. Conclusion

Data privacy and security are major concerns in sports, particularly with the rising use of technology and data - driven techniques, which necessitates attention from sports organisations, athletes, staff, and fans. Athletes' sensitive data, including health records, performance data, and personal information, must be safeguarded against unauthorised access, misuse, or theft. Lack of rules, limited resources, inadequate education and awareness, and the advent of new risks and vulnerabilities are among the difficulties confronting data privacy and security in sports.

There are numerous solutions to these challenges, including the implementation of regulations pertaining to data protection, the enhancement of security measures, the provision of education and training programmes, the conduct of frequent risk assessments, and collaboration with technology and security specialists. Sports organisations and players may ensure that their data is secure and protected from possible threats or breaches by deploying these solutions. The sports industry may improve data privacy and security, secure sensitive information, and establish trust with stakeholders by applying these solutions and exploring future research areas. Finally, the responsible gathering, storage, and use of personal and sensitive information in sports will help to ensure the integrity and fairness of sporting events, as well as the trust of athletes, staff, and fans.

## References

[1] Stefan Razvan Tataru, Irene Teodora Nica, Privacy & Data Protection in Sport Industry, SPORT AND SOCIETY Interdisciplinary Journal of Physical Education and Sports, (2020)

[2] C. Burt, “Athletes data privacy concerns raise question of what counts as biometrics” biometricupdate. com, May 17, 2022. [Online]. Available: https: //www.biometricupdate. com/202205/athletes - data - privacy - concerns - raise - question - of - what - counts - as - biometrics#: ~: text=%E2%80%9CBiometric%20Data%20is%20data%20or, %2C%E2%80%9D%20the%20NWSL%20CBA%20reads.

[3] T. Holmes, “Data collection in Australian sport leading to privacy issues for athletes”, abcnews, Apr.15, 2022. [Online]. Available: https: //www.abc. net. au/news/2022 - 04 - 15/data - collection - in - australian - sport - leading - to - privacy - issues/100993950.

[4] Editor, “The Importance of Data Privacy in Sports Management”, isports, Oct.6, 2022. [Online]. Available: https: //isportz. co/the - importance - of - data - privacy - in - sports - management/#: ~: text=To%20achieve%20on%2Dfield%20success, financial%20losses%20and%20legal%20problems.

[5] H. Redlich, “ Australia: Data protection in sport: Legal obligations when collecting athletes data (Part 1) ”, mondaq, May, 7, 2022. [Online]. Available: https: //www.mondaq. com/australia/data - protection/1190968/data - protection - in - sport - legal - obligations - when - collecting - athletes - data - part - 1.

[6] R. Brian, “Game - Changing Wearable Devices that Collect Athlete Data Raise Data Ownership Issues”, leob & leob llp, July, 2017. [Online]. Available: https: //www.loeb. com/en/insights/publications/2017/07/game - changing - wearable - devices - that - collect - athl__ .

[7] General Data Protecting Regulation, ARTICLE 29.

[8] K. Gallagher, “Game On – Tackling the threat of a data breach in professional sports”, endpoint protector, Mar.23, 2023. [Online]. Available: https: //www.endpointprotector. com/blog/game - on - tackling - the - threat - of - a - data - breach - in - professional - sports/.

[9] L. Gia, W. Fan, “Medical Sports Data Privacy Protection Method Based on Legal Risk Control”, J Healthc Eng, May 8, 2021. [Online]. Available: https: //www.ncbi. nlm. nih. gov/pmc/articles/PMC8128551/ .

[10] M. Greenwald, “Cybersecurity in Sports Questions of Privacy and Ethics”, Tufts Univ., Dec., 2017.

[11] D. Manek, J. Gray, “Monetizing Sports Data and Protecting Athlete Privacy: Where is the Balance?”, lexology, Feb.9, 2023. [Online]. Available: https: //www.lexology. com/library/detail. aspx?g=4831cffa - 3b9a - 4ff6 - 8353 - 1a80edf22955

[12] National Youth Sports Institute, “Personal Data Protection Policy (Youth Athletes/Parents/Guardians) ”, NYSI, Available: https: //www.nysi. org. sg/about - nysi/personal - data - protection - policy - youth - athletes - parents - guardians

[13] S. Dasguptha, S. Reddy, “Putting the Athlete First: Data Protection in Sports”, thebastion, Aug.17, 2019. [Online]. Available: https: //thebastion. co. in/politics - and/sports/putting - the - athlete - first - data - protection - in - sports/

[14] K. Karkazis, JR. Jennifer, “Tracking U. S. Professional Athletes: The Ethics of Biometric Technologies”, American Journal for Bioethics, Jan.17, 2017, Available: https: //pubmed. ncbi. nlm. nih. gov/27996918/

[15] R. L. Kathryn, S. Andrew, “Sports Betting and Data Security: Cybersecurity, Data Protection, and Privacy Rights in Gaming Law Practice”, businesslawtoday, Feb.10, 2021. [Online]. Available: https: //businesslawtoday. org/2021/02/sports - betting - data - security - cybersecurity - data - protection - privacy - rights - gaming - law - practice/