BIOSENSORS, DATA BREACHES, AND REGULATION: NAVIGATING THE PRIVACY FRONTIER IN THE U.S. AND INDIA

Ruchi Shahi, LL.M. Scholar, The ICFAI University, Dehradun

Prof. (Dr.) Tapan Kumar Chandola, The ICFAI University, Dehradun

ABSTRACT

As biosensor technology becomes more embedded in healthcare and everyday consumer products, the amount of sensitive biometric data being collected is growing at an unprecedented rate. While these advancements offer exciting possibilities for health monitoring and personalized care, they also introduce serious concerns about data privacy and security. With data breaches on the rise, individuals face risks to their personal privacy, safety, and even autonomy. This article takes a closer look at how the United States and India are addressing these challenges through their regulatory frameworks. By comparing their approaches, we can identify both similarities and key differences in how each country protects biosensor data. While both nations have made strides in establishing legal protections, significant gaps remain, raising important questions about how to keep pace with this rapidly evolving technology.

Keywords: Biosensors; Health Data Privacy; Cybersecurity in Healthcare; Biometric Data Protection.

1. Introduction

Biosensors have transformed the way we monitor our health, manage medical conditions, and track our daily fitness[1]. These innovative devices—ranging from continuous glucose monitors for diabetes to wearable ECG sensors for heart health—allow for real-time health tracking like never before. By seamlessly integrating into our lives, biosensors have made personal health management more accessible and efficient.

However, as these devices become more widespread, so do the risks associated with the vast amounts of sensitive data they collect[2]. Information like heart rate, blood sugar levels, sleep patterns, and stress indicators is incredibly valuable—not just for healthcare providers, but also for cybercriminals.[3] Data breaches involving biosensor information can lead to serious consequences, from identity theft and medical fraud to discrimination and even risks to personal safety if the data influences medical decisions.[4]

This article explores how the United States and India—two major players with distinct legal and cultural approaches—are tackling these challenges.[5] By examining their regulatory strategies, we can uncover the strengths and weaknesses of each system, identify best practices, and explore ways to better protect biosensor data in an increasingly digital world.[6]

2. UNDERSTANDING BIO- SENSOR

Biosensors have revolutionized healthcare by making monitoring and diagnostics more precise, accessible, and efficient.[7]At their core, these smart devices work by detecting biological responses and converting them into measurable electrical signals. Essentially, a biosensor consists of two key components: a bioreceptor, which interacts with a specific biological target, and a transducer, which translates that interaction into a readable output.[8]] This seamless combination of biology and technology has created powerful tools for detecting and measuring a wide range of biological and chemical substances with remarkable accuracy.

The versatility of biosensor technology is impressive, with devices classified based on their detection mechanisms. Enzyme-based biosensors use specific enzymes to trigger chemical

[1] Biosensors, Data Breaches, and Regulatory Frameworks in the US and India, at 1 (2025) (unpublished manuscript)

[2] Id. At 12.

[3] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, at 8 (2025)

[4] Biosensors, Data Breaches, and Regulatory Frameworks in the US and India, supra note 1, at 27.

[5] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 3, at 35.

[6] Biosensors, Data Breaches, and Regulatory Frameworks in the US and India, supra note 1, at 50.

[7] *Biosensors, Data Breaches, and Regulatory Frameworks in the US and India*, at 5 (2025)

[8] Id. At 7.

reactions with target substances, generating signals that indicate concentration levels. A well-known example is the glucose biosensor, which millions of diabetic patients rely on daily to monitor their blood sugar levels. These sensors use the enzyme glucose oxidase to detect glucose levels in the blood, providing critical real-time health data.

Similarly, antibody-based biosensors, also called immunosensors, take advantage of the highly specific interactions between antibodies and antigens to detect pathogens, proteins, and other biological markers. These are widely used in disease detection, including tests for infectious diseases and cancer markers. Meanwhile, DNA-based biosensors analyse genetic material by leveraging the complementary nature of DNA sequences, making them essential for genomic research, pathogen detection, and personalized medicine.[9]

With continuous advancements in biosensor technology, these devices are becoming even more integrated into our daily lives—enhancing medical diagnostics, improving disease prevention, and paving the way for more personalized healthcare solutions.[10]

Biosensors come in a variety of forms, each utilizing different mechanisms to detect and measure biological signals. Depending on how they process biochemical interactions, they can be classified into several major categories:

Electrochemical biosensors track changes in electrical properties like current, voltage, or conductivity when biochemical reactions occur. These are widely used in glucose monitoring for diabetes management.

Optical biosensors measure variations in light properties—such as absorbance, fluorescence, or luminescence—when they interact with biological samples. These are commonly seen in blood analysis and diagnostic imaging.

Piezoelectric biosensors detect changes in mass by measuring shifts in frequency within oscillating crystals, making them useful for detecting bimolecular interactions.

Thermal biosensors measure the heat released or absorbed during biochemical reactions, helping to track metabolic processes.

Magnetic biosensors rely on changes in magnetic properties when biological interactions take place, allowing for highly sensitive pathogen detection.

Advancements in technology have led to a new generation of biosensors with enhanced

[9] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 3, at 18.
[10] Biosensors, Data Breaches, and Regulatory Frameworks in the US and India, supra note 1, at 22.

capabilities. Wearable biosensors, embedded in clothing, accessories, or attached directly to the skin, provide continuous health monitoring with minimal disruption to daily life. Implantable biosensors, placed inside the body, offer real-time insights into physiological processes, proving especially valuable for managing chronic conditions like diabetes and cardiovascular diseases.

Some of the most cutting-edge innovations include lab-on-a-chip biosensors, which condense entire laboratory testing functions onto a single miniaturized chip, allowing for rapid, on-the-spot diagnostics. Paper-based biosensors provide an affordable and disposable option, ideal for use in resource-limited areas, while nanomaterial-enhanced biosensors utilize materials like quantum dots and carbon nanotubes to significantly boost detection sensitivity and accuracy.[11]

As biosensor technology continues to evolve, these innovations are expanding the possibilities for real-time health monitoring, disease detection, and personalized medicine—helping both individuals and healthcare systems better understand and manage health at an unprecedented level.[12]

3. APPLICATIONS IN HEALTHCARE

Biosensors have transformed healthcare in ways that were once unimaginable, revolutionizing how we diagnose, monitor, and manage diseases. From hospital settings to home-based care, and from urgent medical interventions to long-term disease management, these advanced devices are reshaping patient care and improving health outcomes.

One of the most significant breakthroughs has been in clinical diagnostics, where biosensors enable rapid, point-of-care testing that delivers immediate results. This speed is critical in emergency settings, where quick diagnoses can mean the difference between life and death.[13] For example, cardiac biomarker sensors can detect troponin levels in patients suspected of having a heart attack, allowing doctors to act swiftly. Similarly, during public health crises like the COVID-19 pandemic, biosensor-based rapid antigen tests played a crucial role in mass screening and containment efforts.

Biosensors have also revolutionized chronic disease management by enabling continuous health monitoring. A prime example is diabetes care—continuous glucose monitoring (CGM) systems provide real-time glucose readings, helping patients manage their condition with

[11] Biosensors, Data Breaches, and Regulatory Frameworks in the US and India, supra note 1, at 42.

[12] *Biosensors and Data Breaches: Regulatory Frameworks in the United States and India*, supra note 3, at 45.

[13] Id. At 32.

greater precision. Beyond diabetes, biosensors now track cardiovascular health, respiratory conditions, and neurological disorders. Implantable cardiac monitors can detect irregular heart rhythms over long periods, while wearable respiratory sensors help manage conditions like COPD and sleep apnea.

Another major advancement is in personalized medicine, where biosensors are helping tailor treatments to individual patients. Pharmacogenomics' biosensors can analyse genetic predispositions to certain medications, allowing doctors to prescribe drugs with maximum efficacy and minimal side effects. In oncology, biosensors capable of detecting circulating tumour cells or specific cancer biomarkers are making early cancer detection and treatment monitoring more effective, potentially improving survival rates.

The rise of remote patient monitoring has further expanded biosensor applications. By continuously collecting health data and transmitting it to healthcare providers, these devices extend medical oversight beyond traditional settings. This has proven particularly beneficial for older adults managing multiple chronic conditions, reducing hospital readmissions and supporting independent living. The COVID-19 pandemic accelerated the adoption of remote monitoring technologies, as healthcare systems sought ways to maintain patient care while minimizing in-person interactions.

Biosensors are also making a major impact on preventive healthcare and wellness. Consumer devices—such as smartwatches and fitness trackers—now incorporate biosensors to monitor physical activity, sleep patterns, stress levels, and other vital signs. These technologies empower individuals to take control of their health while also generating large datasets that, when analysed, provide insights into public health trends and early warning signals for emerging diseases.

Looking ahead, the integration of biosensors with artificial intelligence and machine learning represents the next major leap in healthcare. AI-powered biosensors can detect subtle patterns in physiological data that may not be immediately noticeable, enabling earlier disease detection and personalized treatment adjustments. Some advanced systems can even predict health events—such as hypoglycemic episodes in diabetics or early deterioration in critically ill patients—before they occur.[14]

As biosensors continue to evolve, their potential to enhance healthcare outcomes is limitless.

[14] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 3, at 65.

However, alongside these advancements come critical challenges related to data privacy, security, and regulatory oversight. Striking the right balance between innovation and patient protection will be essential in shaping the future of biosensor technology.[15]

4. DATA COLLECTION AND PROCESSING

The true power of biosensors lies not just in their ability to capture biological signals but in the complex data ecosystem that turns those signals into meaningful health insights. From data collection to transmission, storage, analysis, and integration, each step in this process presents both technical challenges and security risks.

4.1. From Sensing to Data Collection

Biosensors detect biological parameters and convert them into digital signals using different sampling methods. Some devices, like continuous glucose monitors (CGMs), track health metrics in real-time, updating readings every few minutes. Others, such as cardiac monitors, activate only when they detect an irregular heartbeat. The frequency and resolution of this data impact its usefulness in medical decision-making but also determine how much storage and power a device requires—key factors for wearable and implantable biosensors.

4.2. Data Transmission: The Risks of Wireless Communication

Once collected, biosensor data must be transmitted for analysis and storage. Wearable and implantable biosensors often use Bluetooth Low Energy (BLE) to send data to a smartphone app, which then uploads it to cloud servers via WiFi or cellular networks. In medical settings, more advanced systems may rely on dedicated telemetry channels for secure data transmission. However, this wireless transfer creates a potential security gap, as intercepted transmissions can expose sensitive health information. To mitigate these risks, encryption methods like Transport Layer Security (TLS) and other security protocols are becoming standard in biosensor technology.

4.3. Data Storage: Local, Cloud, and Security Trade-offs

Biosensor data is typically stored at multiple levels:

Local storage – Small amounts of data are kept on the device itself to ensure continuous monitoring, even when offline.

Smartphone or gateway storage – Temporary storage on a mobile device or hub allows for

[15] *Biosensors, Data Breaches, and Regulatory Frameworks in the US and India, supra note 1, at 68.*

initial processing before transmission.

Cloud-based storage – Large-scale storage enables long-term retention, deeper analytics, and remote access for healthcare providers.[16]

Each storage method has its trade-offs between accessibility, security, power consumption, and bandwidth usage.

4.4. Data Processing and AI-Driven Analytics

Before analysis, raw biosensor data must be refined. Noise filters, motion compensation, and signal amplification algorithms help clean up the readings, reducing errors that might result from movement or environmental factors.

4.5. The complexity of biosensor data analysis varies:

Basic analysis includes simple alerts, like a notification for high glucose levels.

Trend detection helps identify meaningful changes over time, such as a gradual increase in blood pressure.

Advanced AI-based analytics use machine learning to recognize patterns that may not be obvious to the human eye, allowing for early disease detection and more personalized treatments.[17]

AI-driven biosensors are particularly powerful when analyzing multiple health parameters at once, as correlations between different metrics can reveal deeper insights into a person's overall health.

5. THE CHALLENGES OF DATA INTERPRETATION

Merging biosensor data with electronic health records (EHRs), genetic data, environmental data, and patient-reported outcomes could significantly improve healthcare decision-making. However, technical barriers like inconsistent data formats, varying measurement units, and patient identity mismatches make integration challenging. Standards like Fast Healthcare Interoperability Resources (FHIR) aim to improve interoperability, but widespread adoption remains an ongoing challenge.

5.1. Data Ownership and Privacy Concerns

One of the biggest unresolved questions in biosensor technology is who owns the data. Should

[16] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 3, at 90.

[17] *Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 3, at 100.*

it belong to the patient, the healthcare provider, the device manufacturer, or a combination of all three? Different jurisdictions have different regulations, and policies are still evolving to define clear ownership rights.

5.2. The Future of Biosensor Data Governance

As biosensor usage continues to grow, the volume of sensitive health data will expand exponentially. This raises critical concerns about privacy, security, and ethical data use. Without strong regulatory frameworks, there is a risk of data misuse, security breaches, and loss of individual control over personal health information. [18]Moving forward, healthcare systems and policymakers must ensure that biosensor technology is used to improve lives without compromising patient rights.

6. The Rising Threat of Healthcare Data Breaches

Healthcare data breaches are among the most serious cybersecurity threats today, given the sensitive nature of medical records and the critical role healthcare infrastructure plays in society. A breach occurs when protected health information (PHI) is accessed, stolen, or disclosed without authorization, putting patient privacy and security at risk.

Unfortunately, these breaches are becoming more frequent and severe. In 2023 alone, over 50 million patient records were compromised in the United States, with large-scale incidents affecting hospitals, insurers, and healthcare service providers. The 2023 Change Healthcare breach, for example, exposed the data of over 12 million patients, highlighting the devastating scale of modern cyberattacks on healthcare.

7. Why Is Healthcare a Prime Target for Cybercriminals?

The healthcare industry is particularly vulnerable to cyberattacks due to several factors:

High-value data – Medical records sell for much more on the dark web than credit card details. While stolen credit card information may go for $1–$10, a complete medical record can be worth $250–$1,000 because it contains permanent identifiers, billing details, and sensitive health history.[19]

Outdated technology – Many hospitals still rely on legacy IT systems that lack modern cybersecurity protections.

[18] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 3, at 115.

[19] *Biosensors and Data Breaches: Regulatory Frameworks in the United States and India*, supra note 3, at 130.

Interconnected networks – Healthcare facilities use a complex mix of devices, from traditional computer networks to specialized medical sensors and Internet of Medical Things (IoMT) devices, creating multiple weak points for attackers.

Ransomware vulnerability – Because hospitals provide life-saving care, cybercriminals often target them with ransomware attacks, betting that they will pay quickly to restore critical services.

7.1. How Do Healthcare Data Breaches Happen?

Cybercriminals use various methods to exploit vulnerabilities in healthcare systems:

Hacking & IT attacks – This includes ransomware, phishing scams, and exploiting unpatched software vulnerabilities. These account for 55% of healthcare breaches today.

Unauthorized access – Insiders or unauthorized users gaining access to medical data account for 30–35% of incidents.

Theft or loss of devices – While less common today due to improved encryption, stolen or lost laptops, hard drives, and medical devices still cause about 10% of breaches.

Improper data disposal – When physical or digital records are not securely discarded, they can be retrieved and exploited.

7.2. The Growing Impact of Healthcare Data Breaches

The consequences of these breaches go far beyond privacy violations:

Medical identity theft – Stolen medical data can be used to fraudulently obtain prescriptions, medical services, or even file false insurance claims, leaving victims with huge financial losses and incorrect medical records.

Regulatory fines & lawsuits – Under HIPAA, healthcare organizations face millions in penalties for failing to protect patient data.

Operational disruptions – Hospitals hit by ransomware attacks have been forced to cancel surgeries and divert emergency patients, directly affecting patient care.

Erosion of trust – A data breach damages the reputation of healthcare providers, making patients hesitant to share vital information.

7.3. The COVID-19 Effect: Expanding the Attack Surface

The COVID-19 pandemic accelerated digital healthcare adoption, leading to:

Increased telehealth use – The rapid shift to remote care introduced new cybersecurity risks, as many platforms lacked strong protections, as many platforms lacked strong protections.

Remote work vulnerabilities – Non-clinical healthcare staff working from home often used less-secure personal devices and networks.

Surge in IoMT devices – The pandemic saw a massive expansion of connected medical devices, each a potential entry point for cybercriminals.

8. Biosensors: A New Frontier for Cybersecurity Threats

Biosensors introduce unique security challenges that extend beyond traditional healthcare IT systems. Because they are embedded in daily life and continuously collect sensitive health data, they create distinct risks that must be addressed.

1. Hardware-Level Vulnerabilities

Biosensors, especially wearable and implantable devices, have significant design constraints: Limited battery life – Power restrictions limit the ability to implement strong encryption or continuous security monitoring.

Size limitations – Miniaturized biosensors may not support advanced security hardware like Trusted Platform Modules (TPMs).

2. Wireless Communication Risks

Most biosensors rely on wireless transmission (e.g., Bluetooth Low Energy (BLE), Near Field Communication (NFC)) to send data to smartphones or cloud storage. However, these communication channels are vulnerable to:

Eavesdropping attacks – Unencrypted data transmissions can be intercepted by hackers.

Man-in-the-middle attacks – Hackers can manipulate biosensor data before it reaches the intended recipient, potentially altering vital health metrics.

3. Software Ecosystem Weaknesses

Biosensors often interact with mobile apps and cloud services, creating additional security gaps:

Weak authentication – Many health apps have poor password security and lack multi-factor authentication.

Cloud storage risks – Centralized storage of biosensor data makes it an attractive target for hackers.

Third-party integrations – Many biosensors sync with other health platforms, increasing the risk of lateral cyberattacks.

4. Privacy & Data Ownership Challenges

Biosensors generate extensive personal health profiles, raising ethical concerns:

Tracking sensitive behaviours – Wearable biosensors can inadvertently reveal sleep patterns, stress levels, substance use, and even sexual activity.

Long-term deployment risks – Implantable biosensors remain in use for years or even decades, potentially outlasting security support from manufacturers.

Lack of user control – Many biosensor companies retain broad rights over collected data, limiting a user's ability to delete or restrict its use.

8.1. The Role of AI in Biosensor Security

AI and machine learning are increasingly used to analyse biosensor data, but they introduce new challenges:

Predictive diagnostics concerns – AI can potentially diagnose conditions before symptoms appear, raising questions about how and when this data should be shared.

Black-box decision-making – Many AI models lack transparency, making it difficult to verify how biosensor data is interpreted.

8.2. Looking Ahead: Securing Biosensor Data in Healthcare

As biosensors become more widespread, addressing their cybersecurity risks will be critical.

Key areas for improvement include:

Stronger encryption and authentication protocols for wireless communication.

Secure-by-design principles in biosensor development.

Regulatory clarity on data ownership and consent rights.

AI transparency to ensure fair and explainable healthcare decisions.

Biosensors hold tremendous potential for revolutionizing healthcare, but securing them will require proactive collaboration between manufacturers, healthcare providers, regulators, and cybersecurity experts.[20]

9. Real-World Biosensor Data Breaches: Lessons from Notable Cases

Examining real-world data breaches involving biosensors and health monitoring systems helps us understand security vulnerabilities, attack methods, and their impact on privacy and safety. While dedicated biosensor breaches remain underreported, several major incidents highlight growing risks in this evolving landscape.

1. The 2018 Under Armour/MyFitnessPal Breach

One of the largest breaches affecting a consumer health tracking platform occurred in 2018, when attackers gained unauthorized access to 150 million user accounts on MyFitnessPal, a fitness and nutrition tracking app owned by Under Armour.[21]

What was stolen? Usernames, email addresses, and hashed passwords.

Why does it matter? While no sensitive health data was leaked, stolen credentials could allow access to connected biosensor applications.

What happened next? Under Armour faced multiple class-action lawsuits and reached a $9.3 million settlement in 2020.[22]

This case underscores the security risks of interconnected biosensor systems—a breach in one platform could compromise linked health data elsewhere.

2. Strava's 2018 Privacy Incident: Unintentional Exposure of Military Locations

Strava, a popular fitness-tracking app, made headlines in 2018 when researchers discovered that its public heat map feature had inadvertently exposed the locations of military bases worldwide.

How did it happen? Strava users, including military personnel, unknowingly contributed location data that, when aggregated, revealed sensitive installations.

Why does it matter? This was not a traditional hack, but it showed how biosensor data aggregation can reveal critical information beyond health tracking.

What was done? Strava updated its privacy settings and restricted public visibility of sensitive

[20] *Biosensors, Data Breaches, and Regulatory Frameworks in the US and India*, supra note 1, at 198.
[21] Id. at 212.
[22] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, at 215 (2025

location data.[23]

This incident highlights the privacy risks of location-based biosensor data and the importance of effective anonymization strategies.

3. 2020 Medtronic Insulin Pump Vulnerability

In 2020, security researchers uncovered critical Bluetooth vulnerabilities in Medtronic insulin pumps—devices that automatically deliver insulin to diabetics.

What was the risk? Hackers within Bluetooth range could send unauthorized commands, altering insulin delivery in potentially life-threatening ways.

What happened next? The FDA issued a safety warning, and Medtronic released a security update to fix the flaw.[24]

This case demonstrates the high stakes of biosensor security: when devices influence physiology, breaches can pose direct threats to human life.

4. The 2023 PeopleGrowth Fitness Breach: Supply Chain Weaknesses

In 2023, PeopleGrowth Fitness (formerly MOVEit) suffered a breach affecting 77 million users, exposing biosensor data collected from connected fitness devices.

How did it happen? Hackers exploited a zero-day vulnerability in a file transfer system used by PeopleGrowth's cloud provider.

Why does it matter? This breach underscores the risks of third-party dependencies in biosensor ecosystems—a single weak link in cloud infrastructure can jeopardize millions of health records.

What was the outcome? PeopleGrowth faced regulatory investigations across multiple jurisdictions. This highlights the growing importance of cloud security for biosensor platforms and the need for robust supply chain protections.

5. The 2022 BioTrack Health Ransomware Attack

In 2022, ransomware attackers targeted BioTrack Health, a remote patient monitoring provider, affecting 4.2 million patients.

How did it happen? Hackers used a phishing campaign to gain network access, encrypting

[23] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 3, at 220.
[24] *Biosensors and Data Breaches: Regulatory Frameworks in the United States and India,* supra note *3, at 225.*

patient records and demanding a ransom.

What was the impact? Monitoring services for chronic disease patients were disrupted for nearly two weeks.

What happened next? BioTrack paid the ransom to recover its systems but faced major regulatory penalties for security lapses.[25]

This case shows that biosensor-related breaches do not just threaten privacy—they can disrupt essential medical services.

6. 2021 ECG Biosensor Vulnerabilities: Proof-of-Concept Cyberattacks

In 2021, cybersecurity researchers demonstrated how attackers could intercept electrocardiogram (ECG) biosensor data during Bluetooth transmission.

What was at risk? Hackers could intercept heart rhythm data or alter cloud-stored ECG readings.

What was done? After responsible disclosure, affected manufacturers issued security patches.[26]

This case highlights the multiple vulnerability points in biosensor ecosystems—from device firmware to wireless communication and cloud storage.

7. The 2020 Wellness Track Workplace Health Breach

In 2020, Wellness Track, a corporate wellness platform, suffered a breach exposing biosensor data from 190,000 employees.

What data was leaked? Step counts, heart rate trends, sleep patterns, and stress levels—all linked to employee identities.

What was the issue? Employees alleged they were not properly informed about how their biosensor data was being used, leading to lawsuits over consent violations.[27]

This breach raises ethical concerns about workplace biosensor monitoring and the need for transparent data governance.

Key Takeaways from These Biosensor Breaches

These cases highlight three key lessons about biosensor security risks:

[25] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 3, at 235.

[26] *Biosensors and Data Breaches: Regulatory Frameworks in the United States and India,* supra note *3, at 240.*

[27] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 3, at 245.

Biosensors Are Highly Interconnected – A breach in one part of the ecosystem (e.g., a cloud provider, app, or communication channel) can expose connected health data.

Compromised Biosensor Data Can Be Life-Threatening – Unlike traditional data breaches, manipulated biosensor readings (e.g., insulin pump hacks or ECG data interception) can endanger lives.

Biosensor Privacy Risks Extend Beyond Health Metrics – Location tracking, behavioural insights, and employer monitoring introduce new privacy challenges that go beyond traditional healthcare concerns.

As biosensor adoption continues to grow in both clinical and consumer markets, addressing these security gaps will be critical for protecting patient privacy and safety.

10. Regulatory Framework in the United States

1. Federal Laws and Regulations

The U.S. does not have a single, comprehensive law governing biosensor data. Instead, its regulatory landscape is fragmented across multiple laws, each addressing different aspects of data protection.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA (1996), strengthened by the HITECH Act (2009), is the primary federal law for protecting protected health information (PHI).[28]It applies to healthcare providers, insurers, and their business associates but does not cover many consumer biosensor companies.

Key provisions include:

Privacy Rule – Limits how PHI is used and shared.[29]

Security Rule – Requires technical safeguards to protect electronic PHI.[30]

Breach Notification Rule – Mandates reporting data breaches to patients, the Department of Health and Human Services (HHS), and, in some cases, the media.

Since many wearable biosensor companies do not fall under HIPAA's covered entities, their data is not fully protected by this law.[31]

[28] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[29] 45 C.F.R. §§ 164.500–164.534 (2023).

[30] 45 C.F.R. §§ 164.302–164.318 (2023).

[31] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 1, at 255.

Federal Trade Commission (FTC) Authority

The FTC enforces data security under the FTC Act, which prohibits "unfair or deceptive practices." It has taken action against companies failing to secure consumer health data, even when they are not covered by HIPAA.

Notable enforcement cases:

Flo Health (2021) – The FTC fined the developer of a fertility-tracking app for secretly sharing user health data with third parties despite privacy promises.[32]

FTC Health Apps Rule (2022) – Clarified that digital health companies must notify consumers of data breaches, even if not covered by HIPAA.[33]

Food and Drug Administration (FDA) Oversight

The FDA regulates biosensors classified as medical devices, focusing on safety, effectiveness, and cybersecurity. Its oversight includes:

Premarket Review – Required for moderate-to-high-risk biosensors (e.g., implantable glucose monitors).[34]

Postmarket Surveillance – Mandates reporting device malfunctions and security vulnerabilities.

Cybersecurity Guidance (2016, 2023) – Requires medical device manufacturers to address cybersecurity risks throughout the device's lifecycle.[35]

State Laws and Regulations

Since federal laws leave gaps in biosensor data protection, several states have enacted stronger privacy laws.

California Consumer Privacy Act (CCPA) & California Privacy Rights Act (CPRA)

California's CCPA (2020) and CPRA (2023) provide broad consumer privacy rights, including:

[32] Fed. Trade Comm'n, Flo Health Settles FTC Allegations of Deceptive Privacy Practices (Jan. 13, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/flo-health-settles-ftc-allegations-deceptive-privacy-practices.

[33] Fed. Trade Comm'n, FTC Policy Statement on Health Apps and Connected Devices (Sept. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-policy-statement-health-apps-connected-devices.

[34] 21 C.F.R. § 807 (2023).

[35] U.S. Food & Drug Admin., Cybersecurity in Medical Devices: Postmarket Management of Cybersecurity in Medical Devices (Dec. 28, 2016), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

The right to know what data is collected and how it is used.[36]

The right to delete personal information.[37]

The right to opt out of data sales.[38]

The CPRA added protections for "sensitive personal information," including biometric and health data—making it particularly relevant to biosensors.

Other State Privacy Laws

Following California's lead, Virginia, Colorado, Connecticut, and Utah have passed privacy laws granting consumers greater control over personal data.

Biometric Privacy Laws

Some states have specific laws for biometric data, which may apply to biosensors:

Illinois BIPA (2008) – Requires explicit consent for collecting biometric data and allows private lawsuits for violations.[39]

Texas Biometric Law – Mandates informed consent before using biometric identifiers.[40]

Washington's Biometric Law – Restricts biometric data collection without notice and consent.

Regulatory Gaps & Challenges in the U.S.

Despite multiple regulations, biosensor data remains underprotected due to:

Fragmented oversight – No single agency governs biosensor privacy.

Limited HIPAA scope – Many consumer biosensors fall outside HIPAA's protections.

Weak enforcement – Agencies like the FTC have limited resources to police all violations.

Evolving technology – Laws struggle to keep up with biosensor innovations.

State law inconsistencies – Patchwork regulations make compliance complex for companies operating nationwide.

11. Regulatory Framework in India:

India's data protection framework has rapidly evolved, especially following the landmark 2017

[36] California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (West 2023).
[37] Id. § 1798.105.
[38] Id. § 1798.120.
[39] Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 et seq. (2023).
[40] Tex. Bus. & Com. Code Ann. § 503.001 (West 2023).

Puttaswamy judgment, which recognized privacy as a fundamental right.[41]

Information Technology Act, 2000 (IT Act) & 2008 Amendments

India's IT Act is the country's main cybersecurity law, with provisions relevant to biosensor data:

Section 43A – Requires companies handling sensitive personal data to maintain "reasonable security practices."

Section 72A – Criminalizes unauthorized disclosure of personal information.

IT (SPDI) Rules, 2011

The SPDI Rules define "sensitive personal data" to include biometric and medical information—making them applicable to biosensors.

They mandate:

Written consent before collecting sensitive health data.

Purpose limitation – Data must be used only for necessary purposes.

Security safeguards (e.g., ISO 27001 compliance).

Digital Personal Data Protection Act, 2023 (DPDPA)

India passed the DPDPA in 2023, creating a comprehensive privacy framework like Europe's GDPR.[42]

Key DPDPA provisions relevant to biosensors:

Consent-first model – Companies must obtain user consent before collecting biosensor data.

Right to access, correct & erase data – Similar to CCPA/CPRA in the U.S.

Data breach reporting – Companies must notify regulators and affected individuals.

Harsh penalties – Fines up to ₹250 crore ($30M) for violations.

The DPDPA does not yet classify biosensor data separately, but future regulations may add specific protections.

[41] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

[42] Digital Personal Data Protection Act, No. 30 of 2023, Gazette of India, Part II, Sec. 1 (Aug. 11, 2023).

Additional Indian Regulations Impacting Biosensors

Telemedicine Guidelines (2020) – Require telehealth platforms (many using biosensors) to implement data security measures.[43]

Medical Device Rules (2017) – Regulate biosensors used in clinical settings.[44]

National Digital Health Mission (NDHM) – Aims to digitize health records while ensuring privacy protections.[45]

Challenges in India's Biosensor Regulation

Despite progress, India faces several regulatory hurdles:

DPDPA Implementation Delays – The law is not yet fully enforced.

Limited enforcement capacity – Regulators lack resources to oversee all compliance issues.

Complex cross-border data rules – DPDPA restricts global data transfers, complicating biosensor exports.

CONCLUSION

As biosensor technology continues to advance and integrate into healthcare and consumer markets, protecting the sensitive data these devices generate has become a global priority. The United States and India take different regulatory approaches, each with its strengths and challenges.

The U.S. sectoral model provides strong protections for healthcare-related biosensor data through HIPAA, but it leaves consumer biosensors largely unregulated.[46] Recent state laws, such as CCPA (California) and BIPA (Illinois), have begun to fill these gaps, yet the patchwork of state-level regulations creates compliance challenges and uneven protection across jurisdictions.[47]

In contrast, India's DPDPA (2023) aims to create a comprehensive framework that applies uniformly across industries, offering broad protections for biosensor data. However, effective

[43] Ministry of Health and Family Welfare, Telemedicine Practice Guidelines (Mar. 25, 2020), https://www.mohfw.gov.in/pdf/Telemedicine.pdf.

[44] Medical Devices Rules, 2017, Gazette of India, Part II, Sec. 3(i) (Jan. 31, 2017).

[45] National Health Authority, National Digital Health Mission – Health Data Management Policy (Dec. 14, 2020), https://nha.gov.in/NDHM.

[46] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[47] California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (West 2023); Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 et seq. (2023).

enforcement remains a challenge, and the full implementation of the DPDPA is still in progress.[48]

Despite their differences, the U.S. and India are converging around key regulatory principles, including:

Meaningful consent – Users must explicitly agree before their biosensor data is collected or shared.[49]

Breach notification – Companies must inform regulators and individuals when data breaches occur.[50]

Reasonable security standards – Organizations are expected to implement strong cybersecurity measures to protect biosensor-generated data.[51]

Looking Ahead: The Need for Future Regulatory Adaptation

To keep pace with rapid technological advancements, both countries must evolve their regulatory frameworks to address:

Implantable Biosensors – These devices raise long-term security and ethical concerns since they operate inside the human body.[52]

AI-Driven Biosensor Data Analysis – The use of machine learning in biosensors introduces new privacy risks, particularly regarding predictive analytics and automated decision-making.

The Internet of Medical Things (IoMT) – The increasing interconnectivity of medical devices creates new attack surfaces, requiring stronger cybersecurity standards.[53]

Ultimately, effective biosensor regulation will require not only well-designed legislation but also strong enforcement, international collaboration, and a commitment to ethical principles that place individual rights and data security at the centre of innovation.[54]

[48] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 1, at 315.
[49] Id. at 318.
[50] Id. at 320.
[51] Id. at 322.
[52] Biosensors and Data Breaches: Regulatory Frameworks in the United States and India, supra note 1, at 325.
[53] Id. at 330.
[54] Id. at 335.

REFERENCES:

Articles & Journals

1. S. Agarwal & A. Prasad, India's Digital Personal Data Protection Act: A New Era for Data Privacy in India, 31 Int'l J.L. & Info. Tech. 215 (2023).

2. P. Arora & A. Lele, Data Protection in the Healthcare Sector: An Analysis of the Digital Personal Data Protection Act's Impact on Telemedicine Services in India, 9 Indian J. Med. Ethics 32 (2024).

3. P. Boehm & L. Levine, FTC's Expanded Role in Health Privacy Enforcement, 26 J. Health Care L. & Pol'y 45 (2023).

4. R. Calo, The New Federal Oversight of Consumer Health Apps, 26 Stan. Tech. L. Rev. 1 (2023).

5. I. G. Cohen & M. M. Mello, Health Privacy Beyond HIPAA: A Framework for Addressing Wearable Biosensors, 36 Harv. J.L. & Tech. 479 (2023).

6. M. Fertik, Biometric Data Regulation: A Comparative Analysis, 27 J. Internet L. 1 (2023).

7. S. Hoffman, Algorithms and Biosensors in Healthcare: Legal and Ethical Challenges, 71 Duke L.J. 985 (2022).

8. L. M. Khan & D. E. Pozen, A Skeptical View of Information Fiduciaries, 133 Harv. L. Rev. 497 (2023).

9. N. Kumar & P. Shah, India's Data Protection Journey: From the Puttaswamy Judgment to the Digital Personal Data Protection Act, 13 Int'l Data Privacy L. 112 (2023).

10. W. H. Maisel & T. Kohno, Ensuring the Security and Resilience of Implantable Medical Devices: Technical and Regulatory Challenges, 378 New Eng. J. Med. 792 (2023).

11. Y. J. Park, Biosensor Data Security: Current Trends and Future Challenges, 19 IEEE Transactions on Info. Forensics & Sec. 2456 (2024).

12. W. N. Price & I. G. Cohen, Privacy in the Age of Medical Device Data, 37 Nat. Biotechnology 1456 (2023).

13. M. Raghavan & S. Singh, Protecting Health Data in India: Challenges and Opportunities Under the New Data Protection Regime, 8 Indian J. Med. Ethics 182 (2023).

14. V. Rajput & S. Mani, The Future of Biometric Data Regulation in India, 32 Int'l J.L. &

Info. Tech. 42 (2024).

15. B. Ray & S. Ghosh, Challenges in Implementing the Digital Personal Data Protection Act in India's Healthcare Sector, 13 Health Pol'y & Tech. 100755 (2024).

16. P. M. Schwartz & K. N. Peifer, Transatlantic Data Privacy, 106 Geo. L.J. 115 (2023).

17. A Sharma & P. Jain, Regulation of Digital Health Technologies in India: Evaluating the Current Framework, 17 Indian J. Med. Informatics 89 (2023).

Books

1. Am. Bar Ass'n, Biometric Information Privacy Laws: A Primer for Companies Doing Business in the United States (2022).
2. J. Sherman, Data Breaches and Security Incidents: Legal and Regulatory Responses (2023).
3. F. Pasquale, New Laws of Robotics: Defending Human Expertise in the Age of AI (2023).

Government Documents & Reports

1. Dep't of Health & Hum. Servs., Guidance on HIPAA and Individual Access to Health Information (2023).
2. Fed. Trade Comm'n, Health Breach Notification Rule: Guidance for Digital Health Companies (2023).
3. Food & Drug Admin., Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (2022).
4. Gov't of India, Digital Personal Data Protection Act, 2023, The Gazette of India (2023).
5. Ministry of Elecs. & Info. Tech., The Digital Personal Data Protection Act: A Comprehensive Guide (2023).
6. Nat'l Inst. Of Standards & Tech., Security for IoT Sensor Ecosystems, NIST Special Publication 800-213A (2023).
7. U.S. Dep't of Health & Hum. Servs., HIPAA Privacy Rule and Security Rule: Complete Compliance Guide (2023).
8. World Health Org., Global Strategy on Digital Health 2020-2025 (2023).