International Journal of Reliable and Quality E-Healthcare
Volume 15 • Issue 1 • January-December 2026

Cybersecurity Risks in Medical Devices and Their Impact on Health and Privacy Rights in India

Vidya Menon
https://orcid.org/0000-0002-0855-2788
Gujarat National Law University, India
Received: November 15th, 2025 | **Accepted:** February 3rd, 2026

ABSTRACT

Cybersecurity vulnerabilities in medical devices can have immediate and potentially life-threatening consequences. A successful cyberattack on an implantable device may alter its functioning, disrupt its performance, or disable it entirely, directly jeopardizing the patient's health and safety. Beyond physical harm, these vulnerabilities also endanger informational privacy, as such devices collect, store, and transmit highly sensitive health data. Unauthorized access to such data can lead to exploitation, discrimination, and loss of patient trust in digital health-care systems. Thus, cybersecurity weaknesses simultaneously undermine two deeply interconnected rights—the right to health and the right to privacy—both of which are recognized as integral components of the right to life and human dignity. This paper examines the intersection between medical device cybersecurity and the protection of fundamental rights through a legal and ethical lens. The study emphasizes that digital safety is not merely a technical or regulatory requirement but a moral, ethical, and legal imperative.

KEYWORDS

Digital Health, Patient Safety, Health Care Cybersecurity, Health Data Protection, Right to Health, Right to Privacy, Health Policy India

INTRODUCTION

Fundamental rights derive their true meaning only when interpreted in consonance with changing societal norms and evolving constitutional orders. Health and privacy are two core fundamental rights that are widely recognized not only under international instruments but also within state constitutions. Innovations in the health sector have introduced digital health systems and solutions; however, the emergence of digital health has also exposed systems to multiple cybersecurity vulnerabilities that affect different aspects of the right to life, in particular the rights to health and privacy. Within the realm of digital health, these two are closely interlinked. Today, the right to health is no longer confined to traditional determinants such as clean water, air, and sanitation but extends to the use of digital health technologies for quality health care. Likewise, the right to privacy has evolved beyond its classical notions of home and correspondence to encompass the protection of digital and informational privacy.

Active implantable medical devices (AIMDs) mark a major breakthrough in the field of digital health technologies, offering continuous care through internet connectivity and real-time transmission of medical data to health care professionals, thereby ensuring uninterrupted and personalized patient

DOI: 10.4018/IJRQEH.402039

care. These devices have transformed the lives of millions, enabling them to lead normal lives through continuous device-enabled assistance and constant monitoring for abnormalities. However, the rise in cyberattacks and vulnerabilities targeting health care systems poses a serious threat to care delivery. Since AIMDs are life-sustaining devices, any compromise may directly affect health. Moreover, as health data becomes more valuable and a prime target for adversaries, AIMDs face the risk of unauthorized access to their systems, leading to data breaches and misuse with grave implications for informational privacy. In today's times, the rights to health and privacy therefore call for protection against such vulnerabilities, as without such protection both rights risk being substantially diminished.

Against this background, this article examines the evolutionary and jurisprudential perspectives on the rights to health and privacy, tracing their scope and recognition under international and Indian law through landmark judgments. I further explore the right to health and privacy in the context of digital health, cybersecurity vulnerabilities inherent in AIMDs, and the extent to which such vulnerabilities threaten both health and privacy. Emphasis is also placed on the need for robust medical device cybersecurity practices to safeguard citizens' rights to health and privacy against evolving cybersecurity risks in the health care industry.

INTERNATIONAL POLICIES RELATED TO THE RIGHT TO HEALTH

Health was accorded institutional priority with the establishment of the World Health Organization (WHO) as the United Nations' first specialized agency. In 1946, the *Constitution of the World Health Organization* articulated the right to health by declaring that "the enjoyment of the highest attainable standard of health is one of the fundamental rights of every human being" (World Health Organization, 1946, para.1). The preamble to this constitution further conceptualized health as "a state of complete physical, mental, and social well-being and not merely an absence of disease or infirmity" (World Health Organization, 1946, para. 1). This definition expands the concept of health beyond clinical parameters, closely aligning with the broader notion of overall human well-being. The *Universal Declaration of Human Rights* (UDHR; United Nations, 1948) recognized health as an integral part of the right to an adequate standard of living.

Recognition of the right to health was further reinforced with the adoption of the *International Covenant on Economic, Social, and Cultural Rights* (ICESCR; United Nations, 1966b). The covenant explicitly recognizes "the right of everyone to the enjoyment of the highest attainable standard of physical and mental health" (United Nations, 1966b, Article 12[1]). It further outlines specific obligations that state parties must fulfill to realize this right, including reducing infant mortality, promoting healthy child development, improving environmental and occupational hygiene, preventing and treating diseases, and ensuring access to medical care for all (United Nations, 1966b, Article 12[2]).

The right to health, as codified in the ICESCR, comprises four components: availability, accessibility, acceptability, and quality (Committee on Economic, Social, and Cultural Rights, 2000). Availability refers to the presence of sufficient quantity of functioning health facilities, goods, and services, including hospitals, clinics, trained medical personnel, essential medicines, and access to safe drinking water and sanitation, in line with a state's level of development (Committee on Economic, Social, and Cultural Rights, 2000, para. 12[a]). Accessibility ensures the availability of services to everyone without discrimination, located within a reasonable distance, economically affordable, and supported by access to accurate health information while protecting the confidentiality of personal health data (Committee on Economic, Social, and Cultural Rights, 2000, para. 12[b]). Acceptability means that health care must respect medical ethics, be culturally sensitive, and respond to the specific needs of different populations, including gender and age considerations (Committee on Economic, Social, and Cultural Rights, 2000, para. 12[c]). Quality requires that health services are scientifically and medically sound, are delivered by qualified staff, and use effective medicines and safe, hygienic infrastructure (Committee on Economic, Social, and Cultural Rights, 2000, para. 12[d]). Notably, defining health as a human right emphasizes the necessity of legal accountability, the guarantee of