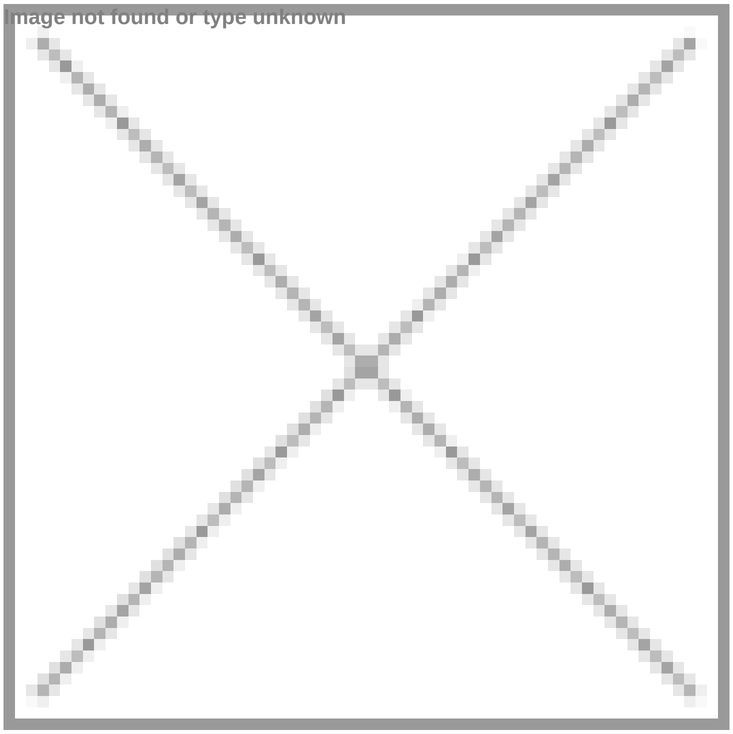
BioSpectrum the business of Bio & Health Sciences

“Healthcare cybersecurity regulations in India are still evolving”

31 March 2026 | Views | By Narayan Kulkarni

As healthcare and pharmaceutical ecosystems become increasingly digital and interconnected, cybersecurity is emerging as a critical priority for the sector. From ransomware attacks on pharmaceutical manufacturing facilities to vulnerabilities in connected medical devices and hospital systems, cyber threats are growing both in scale and sophistication. In this context, organisations are increasingly focusing on strengthening cyber resilience to protect patient data, ensure operational continuity, and safeguard critical healthcare infrastructure. In an interaction with BioSpectrum India, Santosh Jinugu, Partner, Deloitte India, discusses the evolving cybersecurity risks facing the healthcare and pharma sectors, the need for a risk-based approach to cybersecurity investments, and how industry collaboration and initiatives such as cyber simulation labs can help organisations prepare for emerging threats.



What are the major cybersecurity challenges currently facing the healthcare and pharmaceutical sectors?

Over the past few years, the healthcare and pharmaceutical industries have been under increasing cyber pressure. If you go back two or three years, many Indian pharmaceutical companies faced significant ransomware attacks that disrupted production. These were highly targeted incidents, and they exposed the vulnerability of systems that were either legacy or not designed with cybersecurity in mind. Pharma companies operate in a heavily regulated environment—whether it is FDA or other international regulatory requirements—so many of their systems were historically not fully connected or modernised. However, as connectivity increased, cybersecurity was not always integrated into system design. These attacks were a wake-up call for leadership teams and boards, highlighting that cybersecurity is critical not only for business continuity and brand reputation but also for ensuring operational safety.

How is the rise of connected medical devices changing the cybersecurity landscape in healthcare?

Today, we are seeing a rapid increase in connected medical equipment—from devices used in laboratories and emergency rooms to personal healthcare devices. These systems are connected not only to hospital management systems and laboratory information systems but also to broader ecosystems that allow doctors and patients to access information for better diagnosis and treatment. However, many of these devices were not originally designed with cybersecurity as a core component. Hospitals also operate under tremendous operational pressure and are often high-traffic environments, which makes them potential entry points for cyberattacks. Disruptions in diagnostic systems or theft of medical records can have serious consequences. While medical data may not have been viewed as extremely sensitive in India earlier, awareness is growing that patient data protection is critical.

What steps are healthcare and pharma companies taking to strengthen cybersecurity?

Following several high-profile incidents, many organiations have started taking cybersecurity more seriously. Boards and leadership teams are now actively investing in strengthening their cyber resilience. Companies are focusing on improving security at the network perimeter, implementing proactive threat detection, and adopting zero-trust architecture principles. In fact, cybersecurity has increasingly become a regular agenda item in board discussions, with organisations reviewing their cybersecurity posture on a quarterly basis. This shift shows that the industry now recognises cybersecurity as a strategic priority rather than just an IT issue.

Given limited resources, how should healthcare organisations prioritise cybersecurity investments?

Cybersecurity investments should always follow a risk-based approach. Organisations must first identify which systems, divisions, or products are most critical to protect—whether it is patient data, medical devices, or brand reputation. Once risks are clearly understood, companies can prioritise their investments accordingly and gradually enhance their cybersecurity maturity over time. A few years ago, many boards did not have a clear understanding of their top cyber risks. Today, organisations are increasingly adopting enterprise risk management frameworks and cybersecurity standards that provide a holistic view of risks and mitigation strategies.

How is Deloitte supporting healthcare and pharma organisations in strengthening cybersecurity?

We support organisations in multiple ways. At the advisory level, we help companies understand cybersecurity frameworks and implement governance structures that strengthen risk management. At the implementation level, we assist clients in deploying cybersecurity solutions that detect and monitor threats across their systems. In some cases, we also operate cybersecurity services on their behalf—for example, through 24/7 monitoring centres that continuously track potential threats. We also help pharmaceutical manufacturing facilities integrate cybersecurity into their digital transformation journeys, ensuring that cyber considerations are embedded from the beginning rather than added later.

Does Deloitte also provide support for designing secure medical technologies and infrastructure?

Absolutely. Our support spans the entire lifecycle—from the design phase to implementation and managed services. For instance, if a medical device manufacturer is developing a new product, we can help ensure cybersecurity is embedded at the design level. We also work with organisations on securing their network architecture, hospital infrastructure, and manufacturing plants. In addition, we collaborate with various technology partners, including cloud providers such as Google Cloud and AWS. However, our approach is solution-agnostic—we recommend technologies based on the specific needs and environment of the client.

Are there opportunities to work with governments and policymakers on healthcare cybersecurity?

Yes, we work with several government bodies, regulatory agencies, and public sector organisations. Our work includes advising on cybersecurity frameworks, supporting policy development, and assessing the security posture of critical government systems and infrastructure. For example, our teams are also involved in initiatives related to emerging areas like quantum security, helping governments assess risks and prepare future cybersecurity strategies.

Do you believe stronger regulations are needed to improve cybersecurity in healthcare and pharma?

Healthcare cybersecurity regulations in India are still evolving. In many countries, regulations mandate cybersecurity requirements for patient data protection and medical devices. In India, frameworks such as the Digital Personal Data Protection (DPDP) Act exist, but there is still a need for more sector-specific guidance, particularly for connected medical devices and healthcare systems. Often, regulatory changes happen after major incidents. However, the industry should ideally take proactive steps to improve cybersecurity rather than waiting for regulations to enforce it.

How do initiatives like cyber simulation labs help the industry prepare for emerging cyber threats?

Cyberattacks today are complex and layered, often involving multiple systems and actors working together. Simulation environments and cyber labs help organisations visualise how attacks actually unfold in real-world scenarios. By demonstrating these threats and enabling organisations to test their defences, such platforms help build stronger detection, prevention, and response mechanisms. Ultimately, the goal is to educate organisations and strengthen resilience so that they are prepared before a major incident occurs.

Narayan Kulkarni

(narayan.kulkarni@mmactiv.com)