# A Study on Challenges of Data Security and Data Privacy in the Indian Chemical and Pharmaceutical Industry Sector

Angik K. Patel
Swarrnim Startup and Innovation University,
Gandhinagar, Gujarat.

**Abstract**

*The Indian chemical and pharmaceutical sectors have emerged as critical pillars of the nation's economy and global supply chains, with the pharmaceutical industry alone valued at over US$50 billion in 2025. As these industries undergo rapid digital transformation, they face unprecedented challenges in safeguarding sensitive data—ranging from intellectual property and trade secrets to clinical trial data and personal health information. This review article examines the multifaceted data security and privacy challenges confronting these sectors within India's evolving regulatory landscape. It analyzes the intersection of cybersecurity vulnerabilities, compliance obligations under the Digital Personal Data Protection Act (DPDPA), 2023, trade secret protection gaps, and the unique operational risks facing chemical infrastructure. The article synthesizes findings from industry reports, legal analyses, cybersecurity incident data, and policy frameworks to present a comprehensive overview of current challenges and future directions. Key findings reveal that Indian organizations face average data breach costs of Rs. 220 million (US$2.65 million), with pharmaceutical companies experiencing losses exceeding Rs. 22 crore per incident. The review identifies critical gaps in regulatory overlap between cybersecurity and chemical security frameworks, challenges in implementing DPDPA compliance for research data, and structural inequities between multinational corporations and Indian SMEs in trade secret licensing. The article concludes with strategic recommendations for integrating security by design, strengthening regulatory coherence, and building*

*organizational resilience in an increasingly data-driven industrial landscape.*

**Keywords:** *Data security, data privacy, pharmaceutical industry, chemical industry, DPDP Act 2023, cybersecurity, trade secrets, India*

## 1. Introduction

India's pharmaceutical and chemical industries stand at a pivotal moment in their developmental trajectory. The pharmaceutical sector, currently worth more than US$50 billion in 2025 and projected to reach US$130 billion by 2030, supplies a significant portion of the world's generic medicines while driving innovation in specialty chemicals and biotechnology.Concurrently, the chemical industry forms the backbone of India's manufacturing ecosystem, supporting agriculture, pharmaceuticals, and industrial growth through an extensive network of production facilities.This remarkable growth, however, has been accompanied by a parallel reality: data has become the lifeblood of scientific progress, but it is also the most vulnerable asset in these enterprises .

The digital transformation sweeping through these sectors has fundamentally altered the nature of operational risk. Research and development data, clinical trial records, manufacturing processes, customer information, and proprietary formulations now exist primarily in digital form, accessible across global networks and cloud platforms. This digital dependency, while enabling unprecedented collaboration and efficiency, has exposed these industries to sophisticated cyber threats, regulatory complexities, and heightened expectations regarding data protection.

The year 2025 marked a watershed moment for data protection in India with the operationalization of the Digital Personal Data Protection Act, 2023, and the notification of the Draft Digital Personal Data Protection Rules, 2025.This legislative framework introduces stringent obligations for entities processing personal data, with particular implications for pharmaceutical companies conducting clinical trials, contract research organizations managing patient data, and chemical firms handling sensitive commercial information. The Act's consent requirements, purpose limitations, and cross-border transfer restrictions demand fundamental recalibration of how these industries collect, process, and safeguard data.

Simultaneously, the threat landscape has grown more dangerous. According to IBM's 2025 Cost of a Data Breach Report, the average cost of a data breach in India has reached Rs. 220 million (US$2.65 million)—a record high representing a 13% increase over the previous year.Pharmaceutical organizations are particularly exposed, with average losses exceeding Rs. 22 crore per incident.Beyond financial impact, data breaches in these sectors carry profound consequences: compromised intellectual property undermines competitive advantage, exposed patient data erodes trust in clinical research, and cyber-physical attacks on chemical facilities risk catastrophic safety incidents.

This review article aims to provide a comprehensive examination of the data security and privacy challenges facing the Indian chemical and pharmaceutical sectors. It addresses three primary research questions: (1) What are the principal data security vulnerabilities and threat vectors affecting these industries? (2) How does India's emerging data protection framework impact operational practices and compliance obligations? (3) What regulatory and structural gaps exist in protecting sensitive data, and how can they be addressed?

By synthesizing insights from industry reports, legal analyses, cybersecurity incident data, and policy frameworks, this article seeks to inform researchers, industry practitioners, and policymakers about the multifaceted nature of data protection challenges and the strategic imperatives for addressing them.

## 2. The Data Landscape: What Is at Stake

### 2.1 Types of Sensitive Data in Pharmaceutical and Chemical Sectors

Understanding the data protection challenges facing these industries requires appreciation of the diverse and often sensitive nature of the information they handle.

In the pharmaceutical sector, data categories include:

Clinical Trial Data: Clinical research involves processing medical histories, diagnoses, laboratory results, adverse event reports, genetic information, demographic data, and longitudinal health outcomes.This data is inherently sensitive, often revealing intimate details about participants' health conditions and treatments. Even where identifiers are replaced with codes, such data may remain personal if re-identification is reasonably possible.

Genetic and Genomic Data: Particularly sensitive due to its immutability, its capacity to reveal information about family members, and the long-term discrimination risks it carries.While the DPDP Act does not create a separate "sensitive data" category, regulators are likely to treat genetic data as high-risk personal data warranting stricter scrutiny.

Pharmacovigilance Data: Post-marketing surveillance requires long-term retention of patient data and disclosure to regulators, creating ongoing data protection obligations.

Proprietary Research and Formulations: Trade secrets in pharmaceuticals include manufacturing processes, formulas, bioequivalence data, and undisclosed know-how that maintains competitive edge.

In the chemical sector, critical data includes:

Plant Operational Technology (OT) Data: Unlike conventional IT systems, chemical facilities rely on operational technology that controls physical processes. Data from industrial control systems, safety systems, and process automation represents both an operational asset and a vulnerability.

Intellectual Property: Chemical processes, formulations, and manufacturing techniques constitute valuable trade secrets that require protection from industrial espionage.

Supply Chain and Customer Data: Information about suppliers, distributors, and customers creates privacy obligations and commercial sensitivity.

**2.2 The Scale of Data Generation and Associated Risks**

The volume of data generated by R&D labs, clinical trials, and manufacturing environments has grown to unmanageable levels for many organizations. This data explosion creates several interconnected risks:

First, the sheer volume makes comprehensive protection challenging. Organizations struggle to maintain visibility into where sensitive data resides, who accesses it, and how it flows across organizational boundaries.

Second, data aggregation increases the potential impact of breaches. A single incident can expose multiple categories of sensitive information, amplifying harm to data subjects and legal exposure for the organization.

Third, the complexity of modern data ecosystems—spanning on-premises systems, cloud platforms, research collaborations, and global supply chains—creates numerous potential entry points for attackers and multiple pathways for accidental exposure.

### 2.3 Economic and Reputational Consequences of Data Breaches

The financial impact of data breaches in Indian organizations has escalated dramatically. Breach costs have risen by nearly 39% since 2020, with incidents that take more than 200 days to identify and contain costing nearly Rs. 20.5 crore, compared to Rs. 18.4 crore when contained more quickly.

For pharmaceutical organizations specifically, the consequences extend beyond immediate financial loss. Data breaches can invalidate clinical trials, trigger regulatory suspensions, lead to participant withdrawal from studies, and cause irreversible reputational damage.In life sciences, trust is integral to participation and legitimacy—when patients cannot trust that their health data will remain confidential, the entire research enterprise suffers.

For chemical facilities, a cyberattack cannot be mitigated simply by shutting down systems. Unplanned shutdowns can result in chemical leaks, fires, or explosions, worsening an already dangerous situation. The 2017 Triton malware attack on a Saudi Arabian petrochemical plant demonstrated that cyberattacks on chemical facilities can potentially release toxic gases or trigger explosions, risking lives and environmental catastrophe.

India's deep integration into global supply chains compounds these risks. A breach in a single Indian facility can reverberate across international networks of partners, damaging confidence and jeopardizing contracts. In a landscape where reputation and reliability are as critical as cost efficiency, the ability to demonstrate strong security and compliance has become a differentiator in itself.

## 3. Regulatory Framework: DPDP Act 2023 and Its Implications

### 3.1 Overview of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act), represents India's first comprehensive framework for personal data protection. Enacted in August 2023 and operationalized through the Draft Digital Personal Data Protection Rules, 2025, the Act establishes a consent-centric regime governing how organizations may collect, process, store, and transfer personal data.

Key provisions of the DPDP Act include:

Consent Requirements: Consent must be free, informed, specific, unambiguous, and capable of being withdrawn. This standard raises difficult questions in clinical research contexts, where participation may be linked to access to treatment, where data withdrawal may conflict with research integrity, and where consent for future research use may struggle to meet specificity requirements.

Purpose Limitation: Personal data may only be processed for the specific purpose for which consent was obtained. Secondary uses—such as using clinical trial data for AI model training or drug discovery pipelines—require fresh legal justification, often fresh consent.

Data Principal Rights: Individuals gain rights to access, correction, erasure, and grievance redress regarding their personal data.

Cross-Border Transfer Restrictions: Cross-border transfers are permitted only to government-notified jurisdictions. This creates significant challenges for global clinical trials that routinely transfer Indian participant data to global sponsors, central labs, data safety monitoring boards, and regulatory authorities worldwide.

Breach Notification: Data breaches must be reported to the Data Protection Board of India and affected data principals.

Penalties: The Act authorizes penalties up to INR 250 crore per contravention, assessed based on data sensitivity, scale of processing, duration and recurrence, and mitigation measures.

### 3.2 Application to Pharmaceutical and Chemical Sectors

The DPDP Act applies to any entity processing digital personal data, including pharmaceutical manufacturers, biotech companies, contract research organizations (CROs), clinical trial sponsors and investigators, hospitals and trial sites, academic research bodies, pharmacovigilance service providers, and health data analytics platforms.

In the clinical research ecosystem, multiple actors may qualify as data fiduciaries, including trial sponsors who design and control studies and research institutions in certain investigator-initiated trials. CROs, labs, data management vendors, cloud providers, and analytics firms typically act as data processors, processing personal data on the sponsor's instructions.

Crucially, primary compliance responsibility rests with the data fiduciary, even where processing is outsourced. Contractual

delegation does not absolve sponsors of liability. Large pharmaceutical companies and CROs processing sensitive health data at scale may be notified as Significant Data Fiduciaries (SDFs), triggering enhanced governance obligations including data protection impact assessments, periodic audits, and appointment of data protection officers.

### 3.3 The Research Exemption: Scope and Limitations

Section 17(2)(b) of the DPDP Act permits personal data use for research, archiving, or statistical purposes "if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with such standards as may be prescribed". This provision has generated significant discussion within the pharmaceutical research community, with some stakeholders interpreting it as broad immunity from compliance obligations.

However, legal analysis suggests this interpretation is flawed. First, the "standards as may be prescribed" have not yet been notified, meaning the exemption is not yet operational. Second, Indian policy generally restricts exemptions for private, profit-driven research unless a clear public interest is demonstrated. Third, the exemption is likely to be narrowly construed, drawing on parallels with GDPR interpretation that limits research exceptions to non-commercial, public interest research.

Many pharmaceutical entities assume that coded or pseudonymized data falls outside the DPDP Act's scope. This assumption is legally unsafe. Data is anonymized only if re-identification is reasonably impossible, considering available technology and data sets. In many clinical trials, sponsors retain re-identification keys, data is linkable across datasets, and longitudinal tracking is essential—all factors suggesting such data remains personal data subject to full DPDP obligations.

### 3.4 Consent Challenges in Clinical Research

The DPDP Act's consent requirements intersect complexly with existing ethical and regulatory frameworks for clinical trials. Clinical trials in India already require informed consent under the Drugs and Cosmetics Act, ICMR ethical guidelines, and Good Clinical Practice (GCP) standards. However, ethical consent is not automatically equivalent to DPDP-compliant consent.

Several tensions emerge:

Freedom of Consent: Can consent be "free" where trial participation is linked to access to potentially life-saving treatment? The power imbalance between researchers and participants raises questions about whether consent in clinical contexts meets the Act's 高标准.

Withdrawal Rights: How is withdrawal handled once data has been analyzed, published, or shared globally? Research integrity requires maintaining certain data even after withdrawal, creating tension with data principal rights.

Specificity vs. Future Use: Can consent for future, unspecified research be truly "specific"? Legacy consent forms often contain broad future-use clauses that may not meet DPDP standards.

Granularity: The Act's emphasis on specific consent may require more granular permission structures than traditional clinical trial consent forms provide, potentially complicating recruitment and increasing administrative burden.

## 4. Cybersecurity Challenges in Chemical Infrastructure

### 4.1 The Convergence of Cyber and Physical Risk

Chemical facilities occupy a unique position in the cybersecurity landscape because the consequences of successful attacks extend beyond data loss to physical harm. The 2017 Triton malware attack on a Saudi Arabian petrochemical plant marked the first intentional use of malware to cause physical harm—a previously theoretical threat. The malware targeted safety instrumented systems, potentially capable of releasing toxic hydrogen sulphide gas or triggering explosions.

For Indian chemical facilities, this convergence of cyber and physical risk carries particular resonance given the nation's history with chemical disasters. As one analyst notes, if exploited by malicious actors, cybersecurity gaps "can result in another tragedy akin to the Bhopal gas leak incident".

Unlike other industries, a cyberattack on a chemical facility cannot be mitigated simply by shutting down systems. Unplanned shutdowns can result in chemical leaks, fires, or explosions, worsening an already dangerous situation. This creates unique challenges for incident response and requires specialized expertise that integrates cybersecurity knowledge with process safety understanding.

### 4.2 The Regulatory Gap: Chemical Security and Cybersecurity

Despite India's comprehensive cybersecurity governance ecosystem and established chemical security frameworks, the overlap between these two domains remains glaringly insufficient. Table 1 summarizes the existing governance tools:

Cybersecurity National Cyber Security Policy, 2013 Protecting cyberspace information and infrastructure, building capabilities to prevent and respond to cyber-attacks

Cyber Surakshit Bharat Initiative Raising cybercrime awareness and forming safety measures for government IT staff

Indian Cyber Crime Coordination Centre (I4C) Framework for law enforcement to deal with cybercrimes

Cyber Swachhta Kendra Detecting botnet infections and securing end-user systems

CERT-In Collecting and disseminating information on cyber incidents

NCIIPC Protecting Critical Information Infrastructure in power, banking, telecom, transport, government

Chemical Security National Authority for Chemical Weapons Convention (NACWC) Overseeing Chemical Weapons Convention compliance

Chemical Accidents Rules, 1996 Framework for emergency planning and response to chemical accidents

National Disaster Management Authority Coordinating disaster management including chemical accidents

DGFASLI, CPCB, SPCBs Safety regulations, monitoring, occupational health. Source: Compiled from

Critical gaps are evident. Strategic sectors are clustered under critical infrastructure protection, but there is no explicit mention of the chemical and petrochemical industry in the critical infrastructure protection ecosystem. Nor is there any mention of cybersecurity in chemical industry governance frameworks. India's chemical security approach has primarily focused on disaster management and environmental impact, overlooking the potential for intentional cyberattacks.

This gap is particularly concerning given India's experience with cyber threats. The country has seen a 278% increase in state-sponsored cyberattacks between 2021 and 2023 alone, with an

increasing trend of about 3,000 attacks per week even in subsequent months.

### 4.3 Threat Vectors and Vulnerabilities

Chemical facilities face diverse threat vectors that exploit the IT-OT convergence:

Ransomware: Beyond data encryption, ransomware in chemical facilities can disrupt operations, potentially leading to unsafe process states. The 2019 Norsk Hydro attack demonstrated how ransomware could cause major operational shutdowns, leading to over US$70 million in financial losses.

Industrial Espionage: Theft of plant plans, process documentation, and proprietary formulations can undermine competitive advantage and national security.

Phishing and Credential Compromise: These attack vectors remain responsible for almost one in five breaches in India. In chemical facilities, compromised credentials can provide attackers with access to control systems.

Supply Chain Attacks: Third-party vendors, contractors, and software suppliers can serve as entry points into facility networks.

Insider Threats: Disgruntled employees or contractors with legitimate access can cause damage either through malicious action or inadvertent error. Human error remains one of the weakest links in cybersecurity.

## 5. Intellectual Property and Trade Secret Protection

### 5.1 Trade Secrets as Critical Assets

The pharmaceutical industry in India relies heavily on trade secrets to maintain competitive advantage, particularly regarding undisclosed know-how like manufacturing processes and formulas. Unlike patents, which require public disclosure in exchange for limited-term exclusivity, trade secrets can theoretically last indefinitely if adequately protected.

Trade secrets in pharmaceuticals encompass a broad range of information: synthesis processes, purification methods, formulation compositions, quality control procedures, and clinical trial data. This information represents substantial investments in research and development, and its compromise can devastate competitive position.

### 5.2 Intersection of DPDP Act and Trade Secret Protection

The DPDP Act's regulatory regime indirectly affects trade secret protection by focusing on data protection principles, consent

requirements, and safeguards against unauthorized disclosures. The 2025 rules overlap with trade secret protection by categorizing some undisclosed content as personal data, thus affecting licensing contractual relationships where sensitive clinical information and proprietary know-how are traded.

This intersection creates both opportunities and challenges. On one hand, the Act's requirement that data fiduciaries provide reasonable security measures against misappropriation may strengthen protections for data subsets that constitute trade secrets. On the other hand, the classification of certain business information as personal data may create compliance obligations that complicate information sharing in research collaborations.

The proposed Protection of Trade Secrets Bill, 2024, would provide civil remedies including injunctions and damages for misappropriation. However, the relationship between this proposed legislation and the DPDP Act remains unclear, creating a hybrid regulatory framework that may create uncertainty for licensing undisclosed information.

### 5.3 Equity Issues Between MNCs and Indian SMEs

Analysis of joint venture dynamics reveals sharp divergences between Indian SMEs and multinational corporations in pharmaceutical partnerships. Indian SMEs, which constitute over 80% of pharmaceutical firms in India and focus primarily on generics, often enter non-equity alliances or joint ventures with MNCs to access technology. However, they frequently face exploitation through unfair intellectual property terms that give MNCs control over jointly developed secrets.

This inequity manifests in negotiation dynamics. MNCs can leverage global expertise to enforce restrictive non-disclosure agreements that limit SMEs' ability to utilize know-how after joint venture termination. SMEs, with lower R&D budgets (5-7% on average compared to 15-20% for MNCs), lack the legal resources to enforce reciprocal arrangements.

Empirical trends confirm this structural disadvantage. Joint venture dissolutions increased in 2024 as trust deficits spawned litigation, with approximately 20% of pharmaceutical joint venture dissolutions attributed to intellectual property disputes. Without equitable dispute resolution provisions, SMEs remain disadvantaged,

perpetuating a cycle where innovation gains accrue primarily to MNCs.

### 5.4 Judicial Treatment of Trade Secrets

Recent Delhi High Court rulings highlight the need for a coherent legal framework. In a 2024 case, the court awarded an interim injunction against trade secret misappropriation but faced criticism for lacking specificity in identifying what information was protectable. In a biosimilars case, interim protection was granted until July 2025, with the court noting the importance of balancing disclosure and secrecy but refusing to reveal processes to avoid unnecessary publicity.

These rulings, while demonstrating judicial willingness to grant interim relief, also reveal uncertainties in evidentiary standards. The 2025 DPDP rules may help by providing clearer licensing guidance in pharmaceutical partnerships, but judicial inconsistency in applying confidentiality principles remains a challenge.

## 6. Implementation Challenges and Compliance Burdens

### 6.1 Organizational Readiness Gaps

Many pharmaceutical and chemical organizations face significant gaps in their readiness to comply with evolving data protection requirements. These gaps manifest across multiple dimensions:

Awareness and Understanding: Despite the DPDP Act's enactment in 2023, many organizations still lack comprehensive understanding of how its provisions apply to their specific operations. The complexity of applying general data protection principles to specialized research contexts creates particular challenges.

Legacy Consent Forms: Clinical trial consent forms developed before the DPDP Act often fail to meet current standards due to broad future-use clauses, ambiguous data sharing disclosures, and lack of clear withdrawal mechanisms. Retroactively addressing these deficiencies while maintaining research integrity presents significant challenges.

Data Mapping and Classification: Many organizations lack comprehensive inventories of what personal data they hold, where it resides, who accesses it, and how it flows across organizational boundaries. The DPDP Act's requirements for breach notification and consent management necessitate this foundational visibility.

Technical Controls: Implementing access controls, encryption, audit trails, and breach detection capabilities requires investment in

security infrastructure and expertise that many organizations—particularly SMEs—may lack.

### 6.2 Cross-Border Data Transfer Complexities

Global clinical trials depend fundamentally on cross-border data flows. Indian participant data must routinely be transferred to global sponsors, central laboratories, data safety monitoring boards, and regulatory authorities worldwide. The DPDP Act's restriction of cross-border transfers to government-notified jurisdictions creates significant compliance challenges.

Pharmaceutical companies must now map global data flows, monitor Indian government notifications regarding approved jurisdictions, reassess global trial architectures, and consider data localization or segmented storage approaches. Failure to anticipate restrictions could disrupt ongoing trials and delay new drug approvals.

The uncertainty regarding which jurisdictions will be notified compounds planning difficulties. Organizations must develop flexible architectures that can adapt as the notification list evolves, while simultaneously maintaining trial integrity and participant safety.

### 6.3 Secondary Use and AI Development

Clinical data collected for specific trials is increasingly valuable for secondary purposes: secondary analysis, AI model training, drug discovery pipelines, and comparative effectiveness studies. Under the DPDP Act, such secondary uses require fresh legal justification, often fresh consent.

Use of historical clinical datasets to train AI models presents particular risks. Legacy consents may not cover AI applications, data may be repurposed far beyond original intent, and cross-border model training complicates compliance. Assumptions that AI training automatically qualifies as "research" exempt from consent requirements are increasingly vulnerable to legal challenge.

For chemical companies, AI applications in process optimization, quality control, and product development similarly raise questions about data provenance and permissible use. Organizations must develop governance frameworks that enable innovation while maintaining compliance.

### 6.4 Resource Constraints for Small and Medium Enterprises

The compliance burden imposed by the DPDP Act falls disproportionately on smaller organizations. SMEs, which dominate the Indian pharmaceutical landscape in terms of number of firms,

typically lack the legal, technical, and compliance resources available to larger competitors.

Resource constraints manifest in several ways. SMEs may struggle to implement the technical controls required for adequate data protection. They may lack in-house legal expertise to navigate complex compliance requirements. They may find the cost of DPDP compliance—including potential designation as Significant Data Fiduciaries with enhanced obligations—prohibitive.

These disparities raise concerns about market concentration and competitive dynamics. If compliance costs become a barrier to participation in research and manufacturing, larger players with deeper resources may consolidate market position, potentially reducing diversity and innovation in the sector.

## 7. Strategic Imperatives and Future Directions

### 7.1 Integrating Security and Compliance by Design

Forward-thinking organizations increasingly recognize that security and compliance must be embedded into systems and processes from the outset, rather than added as afterthoughts. Modern scientific software platforms can play an important role by embedding audit trails, electronic signatures, access controls, and automated compliance monitoring into day-to-day workflows. This approach—compliance by design, security by default—has become a strategic necessity.

For pharmaceutical and chemical companies, this means moving beyond viewing security as an IT function or compliance as a legal obligation. Instead, organizations must integrate these considerations into research planning, facility design, partnership negotiations, and technology procurement.

### 7.2 Leveraging Artificial Intelligence for Security

Traditional approaches to security—firewalls, static audits, manual monitoring—are no longer sufficient to deal with the speed and sophistication of modern threats. Artificial intelligence and machine learning are beginning to transform the landscape, offering capabilities that move security from reactive defense to proactive strategy.

By analyzing patterns across massive datasets, AI systems can identify anomalies in laboratory processes, user behavior, or network traffic long before they escalate into breaches. They can predict

vulnerabilities by drawing on historical data and emerging trends, allowing companies to address risks before they become crises.

In operational technology environments like chemical facilities, AI can detect anomalies in system behavior that may indicate compromise or impending failure. These predictive capabilities are particularly valuable where traditional security methods may fall short.

### 7.3 Strengthening Regulatory Coherence

The gap between cybersecurity frameworks and chemical security regulations represents a significant vulnerability that requires policy attention. India must adapt and evolve existing cybersecurity frameworks to address the unique challenges critical infrastructure like chemical plants face.

Several strategies could address this gap. First, explicit inclusion of chemical facilities within critical infrastructure protection frameworks would extend cybersecurity requirements to these installations. Second, mandating compliance with standards like ISO/IEC 27001 for chemical industries would establish baseline security expectations. Third, fostering collaboration across sectors—including information sharing about threats and vulnerabilities—would enhance collective defence.

The experience of other jurisdictions offers lessons. The United States' Chemical Facility Anti-Terrorism Standards (CFATS), while expired as of July 2023, provided a model for integrating security considerations into chemical facility regulation. India can learn from both the strengths and limitations of such approaches in designing its own framework.

### 7.4 Building a Culture of Security and Privacy

Ultimately, effective data protection depends on organizational culture as much as technical controls or legal compliance. What distinguishes forward-thinking organizations is not simply their ability to comply with regulations, but their willingness to treat security and compliance as assets rather than burdens.

Building this culture requires leadership commitment and recognition that security and privacy are boardroom priorities, central to business strategy and global reputation. It requires training and awareness programs that help employees understand their role in protecting sensitive information. It requires simulation exercises where employees learn to identify phishing and other cyber threats.

In the global marketplace, demonstrable adherence to rigorous standards is increasingly viewed as a mark of quality and reliability. Companies that build security into their culture earn trust not only from regulators but also from customers, partners, and investors.

## 8. Conclusion

The Indian chemical and pharmaceutical industries stand at a crossroads. Their remarkable growth and global integration have positioned them as leaders in generic medicines, specialty chemicals, and research services. Yet this success has also made them targets for sophisticated cyber threats and subjects of increasingly stringent data protection requirements.

This review has identified several interconnected challenges confronting these sectors. The convergence of cyber and physical risk in chemical facilities creates unique vulnerabilities that existing regulatory frameworks inadequately address. The DPDP Act's comprehensive data protection regime demands fundamental changes in how pharmaceutical companies conduct research, manage consent, and transfer data across borders. Trade secret protection, complicated by gaps in legal frameworks and power asymmetries between MNCs and SMEs, requires attention to ensure equitable innovation ecosystems. Implementation challenges—from legacy consent forms to resource constraints—threaten to overwhelm organizations unprepared for the new regulatory landscape.

Addressing these challenges requires strategic responses at multiple levels. Organizations must embed security and compliance into their operations by design, leveraging AI and other technologies to enhance protection while enabling innovation. Policymakers must strengthen regulatory coherence, closing gaps between cybersecurity and chemical security frameworks while providing clarity on DPDP implementation. Industry associations and educational institutions must foster the talent and culture necessary for sustained attention to data protection.

The stakes could not be higher. The average cost of data breaches continues to climb, and the consequences of failure extend beyond financial loss to patient safety, environmental protection, and national competitiveness. However, organizations that successfully navigate these challenges have the opportunity to set new global standards for secure, privacy-respecting scientific enterprise. They will not only

protect their own futures but will also define India's reputation as a secure, reliable, and innovative powerhouse in the decades to come.

The future of India's pharmaceutical and chemical leadership will not be determined solely by production capacity or cost competitiveness. It will depend on how securely organizations handle their intellectual property, their research data, and their regulatory obligations. In this sense, data security and privacy are not merely compliance requirements or technical challenges—they are strategic imperatives that will shape the trajectory of Indian industry for years to come.

## References

Ajaykumar, S. (2024). Securing India's critical infrastructure: Prioritising cybersecurity in chemical facilities. Observer Research Foundation.

Bio Spectrum. (2025). Can DPDPA's Research Exemption Power Private Sector Breakthroughs? Bio Spectrum.

Donlan, M. (2025). Why pharma and chemicals must treat security and compliance as strategic imperatives. Indian Chemical News.

Ghosh, A. (2026). Navigating Data Protection Compliance in Pharma and Life Sciences Under India's DPDP Regime: Clinical Trial Data, Research Exemptions and Patient Privacy. King Stubb & Kasiva.

Kumari, K. (2024). Reassessing The Data Exclusivity Regime for The Indian Pharmaceutical Industry [Master's thesis]. Victoria University of Wellington.

Lao Động News. (2026). Customer data leaked at India's major pharmacy chain. Lao Động.

Murray, K. (2024). Securing India's critical infrastructure: Prioritising cybersecurity in chemical facilities [LinkedIn post].

Pradhan, A. (2025). The Intersection of Data Protection and Trade Secrets in the Changing IP Landscape in India. Khurana & Khurana.

TechCrunch. (2026). Indian pharmacy chain giant exposed customer data and internal systems. TechCrunch.

World Agrochemical Network. (2025). India PMFAI opposes extension of agrochemical regulatory data protection period. AgroPages.