



CIVIL

The Digital Shift: How NABH and DPDP Acts Are Shaping Healthcare Compliance

AUTHOR Appurv Bhatia, Aardra S Prathap

PUBLISHED 30 June 2025

Introduction

Digital transformation is a necessity in today's healthcare landscape, requiring compliance with rigorous standards like those from the National Accreditation Board for Hospitals & Healthcare Providers (NABH). These guidelines prioritise patient safety, data security, and quality care, making compliance crucial for healthcare providers. Aligning with NABH standards and emerging laws ensures hospitals avoid penalties while enhancing operational efficiency and delivering patient-focused care. Embracing these changes is vital for staying competitive and maintaining trust in a rapidly evolving industry. Let's explore why this alignment matters and what steps should be taken to stay ahead.

Why It Matters?

The transition from paper-based systems to digital health solutions is revolutionising patient care through streamlined operations, improved outcomes, and enhanced data security. However, it also presents challenges in adhering to evolving legal and accreditation standards. Hospitals, which manage large volumes of sensitive patient data, must comply with the DPDP Act, 2023, and meet NABH guidelines where accreditation is sought, to ensure compliance and maintain their responsibilities.

Modern healthcare standards now require that hospitals establish secure information ecosystems that extend beyond basic recordkeeping. Compliance frameworks increasingly mandate digital systems to maintain traceable audit trails, role-based access to patient data, encrypted communications, and structured protocols for how, when, and by whom patient information can be accessed or disclosed. These expectations are no longer optional features but central pillars of accreditation and legal adherence.

Understanding the DPDP Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, introduces transformative rules for handling patient data, focusing on secure processing and individual rights. It covers both digitally created data, such as entries in Electronic Health Records (EHR) systems, and scanned data converted from physical records, requiring the same high standards of security and privacy. Hospitals must implement robust measures to prevent data breaches and unauthorised access while obtaining explicit patient consent for lawful use. Patients are also entitled to access and correct their data, ensuring transparency. Non-compliance could result in hefty penalties of up to ₹250 crore, making adherence essential.

In line with this, hospitals are now expected to ensure that patient data is accessed or shared only with the patient's explicit consent or under specific legal authority. All such requests, whether made by patients, clinicians, or government agencies, must follow uniform and transparent processes, supported by digital systems that track disclosures, record timestamps, and ensure accountability. This not only reinforces privacy rights but also strengthens institutional safeguards against misuse or error.

Setting the Benchmark: Navigating NABH's Digital Health Standards

The NABH has established specific guidelines to ensure that hospitals adopt robust digital health practices. Here's what hospitals need to do:

A. Centralised and Secured EHR Systems

Hospitals must implement EHR systems that consolidate patient data into a secure, unified platform, integrating medical history, diagnostics, and treatment plans. These systems enhance communication and care continuity while incorporating data security measures like encryption and multi-factor authentication.

In addition to unifying records, these systems must be capable of generating time-stamped entries, locking historical data, and maintaining comprehensive access logs. Real-time monitoring of data modifications and role-restricted user access are key features now expected of any compliant healthcare information system. Moreover, hospitals must have a documented protocol for data backup, recovery, and downtime handling to ensure patient safety and legal continuity even during system failures.

B. Accessibility of Patient Data

Ensuring patient data security while maintaining seamless access for authorised users is vital for effective care. Role-Based Access Control (RBAC) minimises unauthorised access, while user-friendly EHR interfaces enable quick, efficient data retrieval

during critical situations.

To meet compliance expectations, hospitals must ensure that only designated personnel can access specific types of data, with built-in mechanisms to record who accessed what, when, and why. Systems must be equipped to generate these reports for audits or dispute resolution, and any inappropriate access must be traceable and subject to disciplinary or legal review.

C. Control of Sensitive Reports

NABH mandates strict protocols for handling sensitive reports like Medical Termination of Pregnancy (MTP) and medico-legal cases, emphasising encrypted storage, audit trails, and secure dissemination policies.

Hospitals are required to establish secure digital storage for such sensitive information, ensuring limited access and clear accountability. Disclosure procedures must include patient authorisation, legal documentation where required, and complete tracking of every transfer or view. This reduces the risk of reputational damage or liability arising from the mishandling of confidential data.

Action Plan for Hospitals

Adopting digital health practices while ensuring compliance can be streamlined with these steps:

- **Implement EHR Systems:** Deploy NABH-compliant EHR systems with robust security, scalability, and regular updates to meet operational and regulatory demands.
- **Secure Records:** Use encryption and Role-Based Access Control (RBAC) to protect patient data, along with secure backups for recovery.
- **Legal Collaboration:** Work with legal teams to ensure digital records are admissible and policies align with the DPDP Act, 2023.
- **Staff Training:** Train staff regularly on EHR use, secure data handling, and compliance requirements.
- **Regular Audits:** Conduct periodic audits to identify vulnerabilities, document findings, and implement corrective actions promptly.

Are Scanned Documents Legally Valid?

Under the Bharatiya Sakshya Adhinyam (BSA), 2023, scanned or digitally created records are valid evidence in legal proceedings only if they meet specific conditions, such as being generated during regular operations and accompanied by certificates of authenticity. Hospitals must detail methods and locations of record creation and use reliable systems with operational logs to ensure credibility. Compliance requires certified systems for data storage, systematic logs, and collaboration with legal teams for authenticity certificates. These measures ensure legal admissibility and strengthen the integrity of hospitals' digital documentation.

Benefits of Compliance

Hospitals adopting digital health compliance benefit from improved patient care, efficient workflows, and streamlined processes. Centralised data systems enhance decision-making and coordination, reducing administrative tasks. Compliance with the [DPDP Act, 2023](#), and NABH standards boosts credibility, minimises legal risks, and ensures regulatory alignment. Robust data security measures protect sensitive patient information, fostering trust and confidence. These advancements establish a foundation for modern, reliable healthcare while transforming operations and patient outcomes. Compliance also promotes institutional resilience by embedding safeguards against data breaches and liability from improper access or incomplete records. When implemented holistically, these frameworks turn data management from a legal risk into a strategic advantage.

Conclusion

As India's healthcare system embraces digital transformation, compliance with standards like NABH and laws such as the DPDP Act and BSA is no longer optional; it is essential for sustainable growth. Hospitals that proactively adapt to these requirements not only avoid hefty penalties but also enhance operational efficiency, strengthen data security, and build patient trust. By aligning with these standards, hospitals position themselves as leaders in delivering secure, efficient, and patient-centric care, ensuring they remain competitive and credible in an evolving healthcare landscape.

For more details, write to us at: contact@indialaw.in

Related Practice Areas

Data Protection and Privacy