BioSpectrum the business of Bio & Health Sciences

Patient Consent - How is it different under medical ethics and data protection?

31 October 2025 | Views | By S. Chandrasekhar, CEO, K&S Digiprotect Services

In the ethical and legal framework of medicine and law, consent has always existed. Within healthcare, it signifies the individual's right to be informed and to choose. However, in the digital era, consent assumes a broader function; it becomes the foundation for lawful processing of personal data. For the pharma and clinical-research sectors, this distinction carries significant implications. The Digital Personal Data Protection Act, 2023 (DPDPA), has redefined how personal and health-related data must be managed. This article explores why consent under data-protection law differs from medical consent, drawing lessons from the irregularities uncovered in the Ahmedabad clinical trials, and outlines the emerging compliance responsibilities under the DPDPA.

In late 2025, the Ahmedabad Crime Branch exposed extensive irregularities in the conduct of clinical drug trials. Investigations revealed that multiple pharmaceutical companies and intermediary clinical research organisations (CRO) had engaged unauthorised agents to recruit volunteers, often offering small sums of money. Most participants were enrolled in trials concurrently, often without medical oversight, full disclosure to the volunteers, adequate sanitation, or safety precautions. Substandard testing practices raised immediate concerns about volunteer safety.

What was initially viewed as a failure of medical ethics soon revealed a deeper structural weakness - the negligent handling of participants' personal data. Every clinical trial generates sensitive information health records, biological samples, test results, and demographic identifiers. When such data is processed without appropriate consent or oversight, the consequences extend beyond physical harm to include reputational damage and social discrimination. A data leak revealing a participant's genetic condition or infertility, for instance, can trigger stigma or even loss of livelihood.

The Ahmedabad case, therefore, highlights not just ethical failure in clinical research, but also systemic disregard for data governance, a gap the DPDPA now seeks to bridge.

Distinguishing between medical and personal data consent

Medical consent flows from the principles of bioethics, particularly autonomy and beneficence. It requires that a patient or participant fully understand the medical procedure, its risks, and its intended benefits before agreeing to undergo it.

Data consent, on the other hand, pertains to what happens to an individual's information, not their body. Under the DPDPA, personal data may be processed only when the individual grants consent that is *free, informed, specific, and unambiguous* . It must follow a clear notice describing what data will be collected, why it is needed, and with whom it will be shared, and the individual must retain the right to withdraw it at any time.

In the context of clinical trials, signing a medical consent form for a procedure does not automatically authorise the processing of related data. Institutions must therefore treat data consent as a separate and perhaps a more important requirement.

Consent in the DPDPA

The DPDPA marks a turning point in India's data-governance landscape. It mandates transparency through multilingual consent notices, grants individuals rights to access and correct their data, and even allows them to nominate representatives in case of death or incapacity.

For healthcare entities and CRO's, this means every stage of data collection from recruitment to publication must comply with explicit consent and privacy standards. Failing to do so is not a mere procedural lapse. It can attract heavy financial penalties of up to Rs 250 crore (Approx $28 million), besides causing reputational harm.

Aware patients and their concerns

Modern patients and volunteers are far more digitally literate than in the past. They research treatments online, compare clinical trials, and demand transparency not only about what is done to them, but also about how their personal data will be used. In this context, informed data consent becomes more than a legal safeguard; it functions as an ethical contract that builds confidence and accountability.

Obtaining such consent benefits all stakeholders. It establishes lawful processing records, enhances participant trust, minimises disputes, and promotes a culture of transparency within research institutions. When data-handling practices are clearly communicated, compliance transforms into credibility.

The DPDPA reflects a shift from viewing personal data as an operational resource to recognising it as an extension of individual identity and thereby her Fundamental Right. Within medicine and research, this translates into a dual responsibility, which is, safeguarding both the physical body and the digital body (personal data) of every participant.

Incidents like the Ahmedabad trials illustrate that privacy is inseparable from ethics. Data protection is not merely about encryption or access controls. It is about trust. Genuine consent today requires both medical understanding and digital awareness. Participants deserve to know not only the treatment being administered but also the fate of their personal information.

Conclusion

India's healthcare and research ecosystem stands at the intersection of ethics and technology. The DPDPA does not displace medical ethics. It reinforces it by extending respect from the physical to the digital domain. The Ahmedabad incident underscores the cost of treating consent as a routine checkbox rather than a moral commitment.

By internalising the principles of informed data consent and digital dignity, healthcare and research institutions can not only ensure compliance but also restore public trust, making ethical research synonymous with responsible data stewardship.

S. Chandrasekhar, CEO, K&S Digiprotect Services

(With inputs from Aman Varma, Senior Manager – Legal and Regulatory Affairs, K&S Digiprotect Services)