DPDP Act Survival Checklist: 5 Steps to Audit Your Patient Consent Forms

Reclaim Your Time. Focus on Patient Care. Build Your Practice.

5 Essential Steps to Audit Your Patient Consent Forms for DPDP Act Compliance

The Digital Personal Data Protection (DPDP) Act, 2023, is transforming how Indian healthcare providers (HCPs) handle sensitive data. The concept of **Consent** is now much stricter and more granular.

Use this checklist to immediately audit both your physical and digital patient consent forms to ensure you minimize compliance risk and protect your practice.

Audit Status: ☐ Compliant / ☐ Needs Immediate Update

Step 1: Verify Consent is Free, Specific, and Informed

The DPDP Act demands a higher quality of consent than previous regulations. It must be a conscious, clear choice, not boilerplate legal jargon.

Audit Question	Compliance Requirement (DPDP Standard)	Status
A. Is consent voluntary?	Is the consent form entirely separate from mandatory service agreements (e.g., admitting to a hospital)? It must be **"Free"**—cannot be conditional on treatment.	☐ Yes / ☐ No
B. Is the purpose clear?	Does the form specify *exactly* what the data will be used for? (e.g., "for clinical treatment," "for sending marketing updates," "for sharing with third-party labs"). Vague consent is non-compliant.	☐ Yes / ☐ No

C. Is the Data Fiduciary named?	Does the form clearly identify the name of your practice/hospital (the **Data Fiduciary**)?	☐ Yes / ☐ No
D. Has a notice been given?	Was the patient provided a separate, clear **Notice** detailing the data being collected *before* they signed the consent form?	☐ Yes / ☐ No

---

Step 2: Ensure Right to Access & Withdrawal is Guaranteed

A major shift under the DPDP Act is the patient's (the **Data Principal's**) right to control their data. Your forms must reflect this right.

Audit Question	Compliance Requirement (DPDP Standard)	Status
A. Is withdrawal easy?	Does the form explicitly state that the patient has the **Right to Withdraw Consent** at any time?	☐ Yes / ☐ No
B. Is the process clear?	Does the form specify *how* a patient can withdraw consent (e.g., "by contacting the Data Protection Officer at [email address]")? The withdrawal must be as easy as giving consent.	☐ Yes / ☐ No
C. Are Data Principal rights listed?	Does your linked Privacy Policy or the form itself list the patient's right to **Correction, Completion,** and **Erasure** of their data?	☐ Yes / ☐ No

---

Step 3: Implement Purpose Limitation & Data Minimization

You can no longer collect data “just in case.” You must only collect data relevant to the stated purpose.

Audit Question	Compliance Requirement (DPDP Standard)	Status
A. Is the data limited?	Are you collecting only the data absolutely necessary for clinical care (e.g., avoiding unnecessary data like secondary personal preferences on a clinical form)?	☐ Yes / ☐ No
B. Are data retention timelines clear?	Does the form/policy state *how long* you will store the data? Data must be deleted once the specified purpose (e.g., 3 years of record-keeping) has been served.	☐ Yes / ☐ No
C. Are secondary uses covered?	If you plan to use data for marketing, research, or sharing with a third-party diagnostic lab, is there a **separate, specific checkbox** for that secondary use? (It cannot be bundled with treatment consent).	☐ Yes / Yes / ☐ No

---

Step 4: Validate Consent for Children (Ages 0-18)

The Act imposes special obligations when processing the data of a child (anyone under 18).

Audit Question	Compliance Requirement (DPDP Standard)	Status
A. Is consent taken from the guardian?	For all patients under 18, is the consent mechanism explicitly geared toward securing consent from the **parent or lawful guardian**?	☐ Yes / ☐ No
B. Is the data processing detrimental?	Are you using any data collection methods (like targeted marketing or behavioral monitoring) that could be considered **detrimental to the well-being of the child**? (This is strictly prohibited).	☐ Yes / ☐ No

---

Step 5: Document and Secure the Consent Record

The record of consent itself must be stored securely and be easily retrievable for an audit.

Audit Question	Compliance Requirement (DPDP Standard)	Status
A. Is the consent auditable?	Are you digitally recording **when** consent was given and **what version** of the policy was shown at that time?	☐ Yes / ☐ No

B. Is the record secured?	Is the consent record stored with the same **high level of security and encryption** as the patient's clinical data? (It must be protected against breaches).	☐ Yes / ☐ No

Final Section: The Most Important Step is Delegation

You have successfully audited your patient consent forms and identified your compliance gaps. If you marked any items in the checklist as "Needs Immediate Update," your practice is currently exposed to unnecessary regulatory risk under the **DPDP Act, 2023**.

The audit process confirms: **You are the clinical expert, not the compliance implementer.** Your time is too valuable to spend navigating website backend settings, technical data audits, and legal jargon.

☐ Take Action Now: Secure Your Practice's Digital Health

Your **Content Audit** and **DPDP Compliance** are now a matter of risk management, not just marketing. Let a specialized partner handle the execution.

We will handle the 90% technical process:

1. **Data Crawling:** Generating the full inventory of every page, link, and content piece.
2. **Compliance Implementation:** Updating privacy policies, fixing non-compliant claims, and establishing the necessary DPDP protocols.
3. **SEO Fixes:** Resolving all 404 errors and technical issues that hurt your authority.

Call to Action (CTA)

Don’t wait for a compliance penalty to force your hand. Use the checklist findings you just completed to prioritize a fix.

Book a Free 15-Minute Digital Risk Strategy Call

- **During this call, we will use your completed checklist to create a prioritized, fixed-price action plan for immediate risk removal.*