WHITE PAPER · 08

Whose Feelings Are These?

Employee emotional data under India’s DPDP Act: what HR may see, why ‘aggregated dashboards’ are still a risk, and a firewall architecture in which the employer sees usage, never content

Dr Atul Aswani; Mumbai Psychiatrist and trained as a Results Coach

Whose Feelings Are These?

Employee emotional data under India's DPDP Act: what HR may see, why 'aggregated dashboards' are still a risk, and a firewall architecture in which the employer sees usage, never content

Not legal advice. This paper is an architectural and policy briefing for CHROs, CISOs and legal counsel. It cites the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protectio

Employee emotional data under India's DPDP Act: what HR may see, why 'aggregated dashboards' are still a risk, and a firewall architecture in which the employer sees usage, never content

CONTENTS

01 Executive summary
02 The problem in India: employee wellness data privacy India
03 Why current approaches fail
04 The emotional-fitness model applied
05 The employer's view versus the learner's view
06 Measurement
07 Implementation
08 One-page checklist the reader can run this week
09 FAQ
10 References

AUTHOR

Dr Atul Aswani; Mumbai Psychiatrist and trained as a Results Coach

PUBLISHED

English edition · emotionapp.in/research/whose-feelings-are-these-dpdp-employee-data

01 Executive summary

Late at night an analyst in Hyderabad types two lines into a wellness app about the appraisal she dreads. Failure to keep reasonable security safeguards over personal data like hers can attract a penalty of up to ₹250 crore under the Schedule to the Digital Personal Data Protection Act, 2023, read with section 8(5) and section 33. The Learner Data Firewall is a two-zone architecture: the Learner Data Zone holds content and stays in India; the Operational Zone sees only pseudonymous usage.

The DPDP Act employee data question is not whether an employer may run a wellness programme. Section 7(i) already allows processing for employment and for a benefit the employee has sought. Payroll, attendance and a count of daily reps are employment operations. Journal text, mood notes and coach-chat content are not: the analyst's two lines are hers. Section 6 requires consent for that content to be free, specific, informed, unconditional and unambiguous. A tick-box buried in the joining papers, signed on day one between the laptop form and the ID photo, fails that test.

DPDP Rules 2025 employer duties are dated. The Rules were notified on 13 November 2025 (G.S.R. 846(E)). Core fiduciary obligations take effect in May 2027. Until then the 2011 IT Rules still class "physical, physiological and mental health condition" as sensitive personal data. A policy that says "HR will not look" is a promise. A Learner Data Firewall is a fact: the employer sees participation, never content.

02 The problem in India: employee wellness data privacy India

A colleague in Pune gets bad news mid-shift. His lead books his cab and carries his bag. She does not read his phone. Indian employers are being asked to do the second thing under the banner of the first.

The Periodic Labour Force Survey reported 61.6 crore employed persons aged 15 years and above in calendar year 2025. That is the pool from which corporate wellness tools draw.

The National Mental Health Survey of India, 2015–16, commissioned by the Ministry of Health and Family Welfare and implemented by NIMHANS, found current mental morbidity of 10.56 per cent among adults. The Survey estimated that about 150 million people needed care and that fewer than 30 million were seeking it. Urban metro current prevalence was 14.71 per cent. Those figures are a decade old. They remain the last nationally representative government survey. They are a reason to treat employee mental health data confidentiality as a first-order control, not a brochure line.

The DPDP Act does not create a special category called "sensitive personal data". The 2011 Rules still do, until section 44(2) of the DPDP Act omits section 43A of the Information Technology Act, 2000 in May 2027. Rule 3 of the 2011 Rules lists "physical, physiological and mental health condition" and "medical records and history" as sensitive personal data. A journal about panic before a board meeting sits next to that line even when the product is non-clinical. CISOs who wait for May 2027 to take the classification seriously will spend the next eight months under the older, stricter label.

Breach volume is not theoretical. CERT-In handled 20,41,360 security incidents in 2024. A Government of India note recorded that CERT-In handled over 29.44 lakh incidents in 2025. IBM's Cost of a Data Breach series put the average organisational cost in India at ₹25.5 crore in 2026, up from ₹22 crore in 2025. That figure is an industry measurement, not a statute. The statute's own number is larger: up to ₹250 crore for a failure of reasonable security safeguards, and up to ₹200 crore for a failure to notify the Board and the affected Data Principal.

The trust problem is older than the Act. People already withhold what they feel at work. A dashboard that claims to be "only aggregated" does not repair that. In a six-person team, aggregation is a courtesy title. Latanya Sweeney's 2000 working paper showed that 87 per cent of the United States population was uniquely identifiable from ZIP code, sex and date of birth. An Indian reporting line is a tighter quasi-identifier than a postal code. Department, gender, week of absence and a single outlier score will do the same work.

Table 1. The Indian exposure, in primary figures

Signal	Figure	Why it matters	Primary source
Maximum penalty for failure of reasonable security safeguards	₹250 crore	Ceiling on a content leak or an unlocked journal store	DPDP Act, Schedule item 1, read with ss. 8(5) and 33
Maximum penalty for failure to notify a personal-data breach	₹200 crore	Separate head; stacks with item 1	DPDP Act, Schedule item 2, read with s. 8(6)
Full operational DPDP obligations	May 2027 (18 months from 13 November 2025)	The runway is short	G.S.R. 843(E); DPDP Rules, r. 1(4)
Employed persons aged 15+, 2025	61.6 crore	Scale of the employee-data surface	PLFS / PIB, 27 March 2026
Current adult mental morbidity	10.56 per cent	Wellness tools sit on a high-sensitivity corpus	NMHS 2015–16, NIMHANS / MoHFW

Signal	Figure	Why it matters	Primary source
People estimated to need care, of whom seeking it	~150 million / fewer than 30 million	Employees already withhold; employer-visible content widens the gap	NMHS 2015–16
Unique identification from three demographics	87 per cent	"Anonymised dashboard" is not a legal defence	Sweeney, 2000
CERT-In incidents handled, 2024	20,41,360	The ambient threat is not small	CERT-In Annual Report 2024
Average organisational breach cost, India, 2026	₹25.5 crore	Industry measurement; the statutory ceiling is higher	IBM Cost of a Data Breach, India 2026

The comparison is the point. The statutory ceiling is ₹250 crore. The last government survey of the emotional load is a double-digit percentage of adults. The employed population is more than 60 crore people. A vendor dashboard that shows "team mood" to a manager is not a small feature. It is a processing purpose that the Act will measure against notice, purpose limitation and security.

03 Why current approaches fail

Three habits dominate the market. Each fails the DPDP test on a different clause.

Aggregated dashboards re-identify small teams

k-anonymity, as Sweeney formalised in 2002, requires that each released record share its quasi-identifiers with at least $k - 1$ others. Indian reporting lines rarely meet that bar. A "team wellbeing index" for a pod of eight, sliced by week, is an equivalence class of one the moment a single person is on leave or a single person is new. The manager does not need a name field. The manager already has the roster.

Purpose limitation under section 8 does not pause because the chart has no surname. If the specified purpose was "offer a voluntary daily-rep programme", a manager-facing mood index is a new purpose. A new purpose needs a new notice and, where section 7(i) does not stretch, a new consent under section 6.

Vendor data offshore

Section 16 of the Act permits processing of personal data outside India except where the Central Government restricts a country or a territory by order. Rule 15 of the 2025 Rules follows that structure. There is no general localisation duty for every fiduciary. Significant Data Fiduciaries may face a tighter rule: Rule 13(4) allows the Central Government to require specified personal data and traffic data to stay in India.

That is the legal floor. It is not a reason to host journal text in another country. Employee wellness data privacy India is a trust product as much as a statutory one. A Learner Data Zone that never leaves India is a design choice stronger

than the Act's default. It also simplifies the conversation with a works committee, a union and a CISO who must answer "where does the diary live?"

A processor contract that allows a parent company in another jurisdiction to train a model on learner content is a purpose change. Section 8(1) keeps the Indian fiduciary liable for what the processor does. Section 8(2) requires a valid contract. "Our global model improves the coach" is not a specified purpose unless the notice said so and the consent was specific.

Consent bundled into onboarding

Section 6(1) requires consent that is free, specific, informed, unconditional and unambiguous, given by a clear affirmative action, and limited to personal data necessary for the specified purpose. Section 6 also requires that withdrawal be as easy as giving consent. Section 6(10) puts the burden of proof on the Data Fiduciary.

An offer letter that says "you agree to the wellness app" is not free. It is a condition of joining. It is not specific, because it does not itemise journal text, mood notes, coach-chat logs and vocabulary scores. It is not unconditional, because the job is the condition. It fails section 5 and Rule 3, which require a standalone notice that itemises the personal data, the specified purpose, the manner of withdrawal, the manner of exercising rights, and the manner of complaining to the Board.

Section 7(i) does not rescue the bundle. The clause covers "the purposes of employment" and "provision of any service or benefit sought by a Data Principal who is an employee." Sought is the verb. A benefit the employee asked for can be delivered without the employer reading it. Payroll does not require the diary. Safeguarding trade secrets does not require the diary. The diary is the benefit. Reading the diary is a different purpose.

Coaching practice makes the same point in plainer words. On the metro home, a sales manager in Noida types three lines about a review that went badly. They belong to her. By morning the feeling has passed, like weather. It does not belong in a personnel file. The statute, for once, says what good coaching already knew.

04 The emotional-fitness model applied

PULL QUOTE

CERT-In handled 20,41,360 incidents in 2024; hoping the diary is uninteresting to an attacker is not a control.

EmotionApp is a non-clinical emotional-fitness coaching platform. Positive-psychology techniques are delivered as countable daily reps. An AI coach can hand off to a human. Delivery is WhatsApp-first. The product is designed for 23 Indian languages. Data is India-resident. The build sits under ISO 9001 and ISO 13485 quality systems, with ISO/IEC 27001 as the information-security control frame.

The product is not a medical device in the clinical sense. ISO 13485 is used here as quality-system discipline for a health-adjacent coaching product: design control, document control, corrective action, supplier control. ISO/IEC 27001 is the information-security discipline for the Learner Data Zone. DPDP Rule 6 maps onto those controls without remainder: encryption, access control, access logs retained for at least one year, backups, processor-contract clauses, organisational measures.

Two-zone firewall

The Learner Data Firewall splits the estate.

Learner Data Zone. Holds content. Journal text, mood notes, coach-chat transcripts, named feelings, free-text reflections, any attachment the learner uploads. Stored in India. Encrypted at rest. Accessible to the learner, to an AI coach acting as a processor inside the zone, and to a human coach only after the learner opens the gate. The employer has no role, no key, no view.

Operational Zone. Holds usage. A pseudonymous operational identifier, a timestamp, a completed-rep flag, a streak integer, a count of distinct emotion-words used that week, a participation flag at team or unit grain only where the cell is large enough to survive a k-anonymity test the vendor publishes. No free text. No scores that function as a proxy for “how this person is”.

The two zones do not share a join key that the employer can use. The operational identifier is not the employee number. The mapping table, if one must exist for billing or licence reconciliation, lives in the Learner Data Zone and is available to the vendor’s India-based data-protection officer, not to the customer’s HRIS administrator.

This is the entrepreneurial moat that can be audited. A policy is a laminated poster by the pantry. A zone boundary with separate keys is a control.

Pseudonymous operational identifiers	Section 2 of the Act defines personal data as data about an identifiable individual. A persistent employee number plus a mood score is personal data. A rotating operational token that the employer cannot reverse is still personal data in the vendor's hands. It is not personal data in the employer's hands if the employer cannot reasonably identify the individual from what it receives. That is the design target. It is not a claim of anonymity. Anonymity is a high bar. Pseudonymity plus non-joinability is the honest one.
Tamper-evident access log	Rule 6 requires access logs and their retention. The Learner Data Zone writes an append-only log for every read of content: who, when, which record class, under which legal basis, with which learner permission. The log is visible to the learner on request under section 11. It is visible to the Board if a complaint is filed. It is not visible to the employer as a browsing tool. A break-glass event — a lawful request, a safety escalation the learner has pre-authorised, a court order — is itself a logged event.
Selective sharing controlled by the learner	The learner may share a summary with a manager, a coach or a family member. That is a new, specific consent under section 6. It is time-bounded. It is withdrawable in the same screen. It does not reopen the rest of the Zone. This is the only "manager view" the architecture permits.
India residency	Content and the mapping table stay in India. Operational aggregates may be computed in India and displayed to the employer in India. Cross-border model training on Learner Data Zone content is off. If a Significant Data Fiduciary designation arrives, Rule 13(4) will not require a rebuild.
Encryption at rest	Rule 6 names encryption, obfuscation, masking and virtual tokens as the first security safeguard. Content is encrypted at rest with keys held in India. Employer administrators do not hold those keys. Processor staff who support the AI coach work inside the Zone under a section 8(2) contract, under least privilege, under the access log.

05

The employer's view versus the learner's view

The statute asks a simple question: who can see what, for which specified purpose, on which ground? Table 2 is the answer the architecture gives. Table 3 is the consent flow that has to sit in front of it.

Table 2. Every data element, and who can see it

Data element	Learner	Human coach (after learner gate)	Vendor DPO / break-glass	Employer HR / manager	Employer CISO (ops only)	Ground
Legal name, employee number	Yes	No	Yes, for rights and incidents	Yes, in the HRIS, not in the app content store	Licence list only	s. 7(i) employment administration
Mobile number used for WhatsApp delivery	Yes	No	Yes	No	No	s. 6 consent for delivery
Language preference	Yes	Yes	Yes	No	No	s. 6
Completed-rep count	Yes	Yes	Yes	Yes, as a unit or licence aggregate	Yes	s. 7(i) benefit sought, purpose-limited
Streak length	Yes	Yes	Yes	Yes, aggregate only	Yes	s. 7(i), purpose-limited
Emotional-vocabulary breadth (count of distinct named feelings)	Yes	Yes	Yes	Yes, aggregate only; no word list	Yes	s. 6 + purpose limitation
Participation flag (active / inactive in period)	Yes	Yes	Yes	Yes, at a grain that survives k-anonymity	Yes	s. 7(i)
Journal text	Yes	Only if the learner opens the gate	Only on logged break-glass	Never	Never	s. 6 only
Mood notes and named feelings (content)	Yes	Only if gated	Break-glass only	Never	Never	s. 6 only
Coach-chat transcript	Yes	Yes, inside the assignment	Break-glass only	Never	Never	s. 6 only
AI-coach prompts and model context drawn from content	Yes (export on request)	Inside the assignment	Break-glass only	Never	Never	s. 6; no secondary purpose
Selective share pack the learner creates	Yes	If addressed	Yes	Only the pack, for the period granted	No	s. 6, time-bounded
Access log of content reads	Yes, on request (s. 11)	No	Yes	Never	Never	s. 8; r. 6

Data element	Learner	Human coach (after learner gate)	Vendor DPO / break-glass	Employer HR / manager	Employer CISO (ops only)	Ground
Mapping table (employee number ↔ operational token)	No	No	Yes	Never	Never	vendor fiduciary duty

Table 3. A consent flow that passes the DPDP test

Step	What the learner sees	Statutory hook	What must not happen
1. Offer, not mandate	"Your employer has paid for a voluntary emotional-fitness programme. You may ignore it. Your standing at work does not change."	s. 6(1) free; s. 7(i) "sought"	Bundling into the offer letter or the HRIS join checklist
2. Standalone notice	Itemised list: mobile number, language, rep counts, journal text, mood notes, chat logs. Specified purposes, one by one. Withdrawal path. Rights path. Board complaint path. Eighth Schedule language option.	s. 5; r. 3	A single "I agree to terms" scroll
3. Separate toggles	Delivery consent. Content-processing consent. Research-and-improvement consent, default off. Selective-share consent, default off.	s. 6 specific and limited to necessary data	One master toggle
4. Clear affirmative action	An unticked box the learner ticks, or a typed "I agree to content processing", in the language the learner chose	s. 6(1)	Pre-ticked boxes; silence as consent
5. Withdrawal as easy as grant	Same screen, same language, same number of taps	s. 6	A ticket to a vendor helpdesk
6. Erasure	On withdrawal or when the specified purpose is no longer served, content is erased from the Learner Data Zone and the processor is caused to erase it	s. 8(7); r. 8	Soft-delete that remains in backups beyond the Rule 6 log-retention need
7. Proof	The fiduciary keeps the notice version, the language, the timestamp, the toggle state	s. 6(10) burden of proof	"Everyone accepted at onboarding"

Section 7(i) can carry the employer's payment for licences and the employer's receipt of participation counts. It cannot carry the employer's appetite for content. Where the two collide, section 6 wins, because the content is not necessary for the employment purpose.

06 Measurement

A dashboard that holds no clinical data is not a thinner product. It is the product the statute allows the employer to see.

What the employer sees:

- Rep counts: how many daily techniques were completed in the licensed population, by week.
- Streaks: how many learners kept a run of days, as a distribution, not a named list.
- Emotional-vocabulary breadth: how many distinct feeling-words the population used. Breadth is a practice metric. It is not a score of distress.
- Participation: active licences, dormant licences, time-to-first-rep.
- Cell-size rule: no unit view where the cell has fewer than a published *k*. If the team has fewer than 10 people, the cell rolls up.

What the employer never sees:

- Journal text, mood notes, named feelings as content, coach-chat transcripts.
- Any label that pretends to be a clinical finding. The product does not produce one.
- Individual rank-order of “how people are”.
- A heat map that lights a single desk.

This is the countable-rep model. Entrepreneurship has a plain version of the same idea. You do not inspect the founder’s diary to know whether the company shipped. You count shipments. HR may count reps. HR may not read what a learner typed at midnight.

Machine-learning practice makes the same cut. You do not train a model on labels you were never licensed to see. An employer-facing model that predicts “flight risk” from journal text is a new purpose, a new notice, and almost certainly a consent the learner will refuse. The architecture refuses it first.

ISO/IEC 27001 treats this as scope. The Learner Data Zone is an information asset with a different classification from the Operational Zone. Access control, key management and logging follow the classification. ISO 13485 treats the same cut as design control: the intended use of the employer dashboard is usage, not content. A change request that adds a manager-visible mood score is a design change with a documented risk file, not a sprint ticket.

07 Implementation

A 90-day plan is enough to put the firewall in place before the May 2027 operational date, and to put the 2011 Rules risk to bed now.

Table 4. Ninety-day plan

Week	Owner	Action	Metric
1	CISO + Legal	Map every wellness vendor: what content they hold, where it lives, who inside the employer can see it today	Inventory complete; gaps listed
1–2	Legal	Write the standalone s. 5 / r. 3 notice in English and the Eighth Schedule languages the workforce actually uses	Notice signed off; translation log
2	CHRO	Separate the programme from onboarding. Confirm in writing that non-participation has no consequence for appraisal, bonus or exit	Policy circular issued
2–3	CISO + vendor	Draw the zone boundary. Confirm India residency of the Learner Data Zone. Confirm encryption at rest and key custody	Architecture letter; data-flow diagram
3	Legal + vendor	Rewrite the processor contract: s. 8(2), no secondary purpose, no offshore training on content, erasure on instruction	Executed addendum
3–4	CISO	Turn off every manager-visible content field and every sub-*k* team dashboard	Zero content fields in employer role
4	CHRO + Comms	Tell the workforce, in plain words, what the employer can see and what it cannot	Open rate; questions logged
4–6	Vendor + DPO	Stand up the access log, the learner export (s. 11), the withdrawal path, the erasure path (s. 8(7))	Four paths tested end-to-end
5–7	CHRO	Re-consent existing users with the new toggles. Do not infer consent from last year's click	Percentage re-consented; percentage declined
6–8	CISO	Table-top a breach: r. 7 clock (Board without delay, detailed update within 72 hours; Data Principals without delay)	Drill record; time-to-notice
7–9	Legal	Decide SDF exposure. If volume and sensitivity could trigger s. 10, plan an India-based DPO, an annual DPIA and an independent audit	SDF memo to the board
8–10	Vendor	Publish the cell-size rule and the operational-identifier design. Remove join keys from employer exports	k published; sample export reviewed
10–12	Internal audit	Audit the two zones against Rule 6 and against Table 2 of this paper	Audit report; open items owned
12	CHRO + CISO + Legal	Board paper: what the employer sees, what it never sees, residual risk, Tele-MANAS signpost	Board minute

The metric that matters at day 90 is not adoption. It is the absence of content in the employer's view, plus a notice and a consent record that would survive section 6(10).

08 One-page checklist the reader can run this week

Run this in one working session, with a laptop open on an HR manager's login. Tick only what you can show, not what you intend.

1. Write down every wellness, coaching or "emotional fitness" vendor that processes employee personal data. Include the unofficial ones managers bought on a card.
2. For each vendor, answer: does any employer role see journal text, mood notes, chat logs or a proxy score for an identifiable person? If yes, switch that role off this week.
3. Confirm where content is stored. If the answer is not "in India", treat that as a board-level risk even if section 16 has not yet restricted the country.
4. Pull last year's onboarding pack. If wellness consent lives inside it, it is not free under section 6. Plan the standalone notice.
5. Count the smallest team for which a dashboard is shown. If the cell is under a dozen, treat re-identification as likely: its manager knows who was on leave the week the score dipped.
6. Ask the vendor for the access log of content reads in the last 90 days. If they cannot produce one, they are not meeting the direction of Rule 6.
7. Ask the vendor who holds the encryption keys for content, and in which country.
8. Ask the vendor whether any model is trained on learner content outside the specified purpose. If the answer is vague, the purpose is already drifting.
9. Name the person who will notify the Board and each affected Data Principal if a journal store is opened. Put the r. 7 clock in that person's runbook.
10. Add one line to the programme page and the WhatsApp onboarding message: participation is voluntary; the employer sees usage, never content; help in a crisis is Tele-MANAS 14416.

If you cannot tick items 2, 4 and 10 by Friday, you do not yet have a firewall. You have a slogan.

09 FAQ

Q1 Can HR lawfully see my journal if the company pays for the app?

No. Section 7(i) covers employment operations and a benefit you sought. It does not make the payer the reader. Journal text needs section 6 consent, specific to content, withdrawable on the same screen. The Learner Data Firewall keeps HR on the usage side of that line. One number: ₹250 crore is the ceiling if safeguards around that store fail.

Q2 Is an “anonymised team dashboard” enough under the DPDP Rules 2025 employer duties?

Not if the team is small. Sweeney’s 2000 paper found 87 per cent unique identification from three demographics. A six-person pod plus a week of absence is a tighter key. Publish a cell-size rule. Roll small cells up. If you cannot, do not show the chart.

Q3 Does “legitimate use” for employment mean we can skip consent for the whole wellness stack?

No. Section 7(i) is real, and it is narrow. Licence counts and participation flags can ride on it. Content cannot. Section 6 still governs any purpose that is not necessary for employment or for delivering the benefit. One number: section 6 lists five qualities consent must have — free, specific, informed, unconditional, unambiguous.

Q4 When do we actually have to be ready?

Core fiduciary duties — notice, consent, security, rights, breach notice — take effect in May 2027, eighteen months after the 13 November 2025 notification. The 2011 Rules still treat mental-health condition as sensitive personal data until that date. One number: 18 months from G.S.R. 846(E).

Q5 **If we never look at content, why do we still carry fiduciary risk?**

Because section 8(1) keeps the fiduciary liable for the processor, and because a leak of a journal store is still a personal-data breach under section 8(6). The firewall cuts the employer's eyes. It does not cut the duty to choose a vendor who can keep the zone shut. One number: 72 hours for the detailed Board update under Rule 7 after the first notice given without delay.

10 References

Primary sources only.

1. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), 11 August 2023. Ministry of Electronics and Information Technology. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
2. The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), 13 November 2025. Ministry of Electronics and Information Technology. https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf
3. Commencement notification, G.S.R. 843(E), 13 November 2025. Ministry of Electronics and Information Technology. https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf
4. Establishment of the Data Protection Board of India, G.S.R. 844(E), 13 November 2025. https://www.meity.gov.in/static/uploads/2025/11/cc217843dc3bcb37b2b05bcc3b4e031f.pdf
5. MeitY hub for the DPDP Rules 2025 and related gazettes. https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa
6. Press Information Bureau, "DPDP Rules, 2025 Notified", 17 November 2025. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf
7. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), 11 April 2011, Rule 3. https://indiankanoon.org/doc/101774797/
8. Periodic Labour Force Survey / Press Information Bureau, employment estimates for persons aged 15 years and above, calendar year 2025 (61.6 crore employed, usual status ps+ss), 27 March 2026. https://pib.gov.in/PressReleasePage.aspx?PRID=2246009
9. Gururaj G, Varghese M, Benegal V, et al. *National Mental Health Survey of India, 2015–16: Prevalence, Pattern and Outcomes*. NIMHANS Publication No. 129. Bengaluru: National Institute of Mental Health and Neuro Sciences, 2016. https://ruralindiaonline.org/media/documents/National_Mental_Health_Survey_of_India_2015-16_Prevalence_Patterns_and_Outcomes.pdf
10. Indian Computer Emergency Response Team. *Annual Report 2024*. https://www.cert-in.org.in/

11. Press Information Bureau / Ministry of Electronics and Information Technology note on CERT-In activity in 2025 (over 29.44 lakh incidents). https://static.pib.gov.in/WriteReadData/specificdocs/documents/2026/jan/doc2026123764501.pdf
12. Sweeney L. *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon University, Data Privacy Working Paper 3, 2000. https://dataprivacylab.org/projects/identifiability/paper1.pdf
13. Sweeney L. "k-anonymity: a model for protecting privacy." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10(5), 2002, 557–570. https://doi.org/10.1142/S0218488502001648
14. ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001
15. ISO 13485:2016, *Medical devices — Quality management systems — Requirements for regulatory purposes*. https://www.iso.org/iso-13485-medical-devices.html
16. ISO 9001, *Quality management systems — Requirements*. https://www.iso.org/iso-9001-quality-management.html
17. Tele-MANAS, Ministry of Health and Family Welfare. https://telemanas.mohfw.gov.in/telemanas-services
18. IBM Security. India Records its Highest Average Cost of a Data Breach, 2026. https://in.newsroom.ibm.com/India-Records-its-Highest-Average-Cost-of-a-Data-Breach-2026

Secondary explainers consulted, not cited above as authority: EY, *India's digital privacy crossroads* (2026) and EY DPDP Act 2023 and Rules 2025 point of view; DLA Piper, employer obligations under India's data-protection regime.

About the author

ABOUT THE AUTHOR

Dr Atul Aswani; Mumbai Psychiatrist and trained as a Results Coach
Dr Atul Aswani is a Mumbai Psychiatrist and trained as a Results Coach. He writes for EmotionApp, a non-clinical emotional-fitness platform built by Tranquilo Meditek Sytems Private Limited, Mumbai. The work sits under ISO 9001 and ISO 13485, with India-resident data and WhatsApp-first delivery in Indian languages. This paper is not legal advice. Crisis support: Tele-MANAS 14416.

HOW TO CITE

Aswani A. Whose Feelings Are These?: Employee emotional data under India's DPDP Act: what HR may see, why 'aggregated dashboards' are still a risk, and a firewall architecture in which the employer sees usage, never content. EmotionApp White Paper 8. Mumbai: Tranquilo Meditek Sytems Private Limited; 2026. https://emotionapp.in/research/whose-feelings-are-these-dpdp-employee-data

LAST UPDATED

Last updated: 22 September 2026

NOTE

EmotionApp is a non-clinical emotional-fitness coaching platform. This paper describes practices, techniques and coaching. It is not therapy, treatment, diagnosis or medical advice.

SAFETY NOTE

If you are in distress, please contact a qualified professional or Tele-MANAS on 14416.