

GRC Interview & Study Guide

HIPAA, GDPR & DPDP

Prepared by **Naresh Thalla Mudhiraj** · thallanaresh.com

Personal learning project. Views are my own and do not represent any employer.

Basic to Advanced · scenario-based questions · practical examples · why each topic matters

Version 2.0 · generated 21 October 2026

US healthcare privacy and security rules, the EU GDPR and India's DPDP Act, plus how privacy applies to AI and health data.

Study material written in plain language. Framework and regulatory details change; always confirm against the official, current publication before relying on them.

HIPAA, GDPR & DPDP

US healthcare privacy and security rules, the EU GDPR and India's DPDP Act, plus how privacy applies to AI and health data.

Q: What is HIPAA and who does it apply to?

Basic

HIPAA (the US Health Insurance Portability and Accountability Act of 1996) includes rules, enforced by the HHS Office for Civil Rights, that protect individually identifiable health information (Protected Health Information, PHI).

- **Covered entities:** health plans, healthcare clearinghouses and healthcare providers that conduct certain transactions electronically.
- **Business associates:** organisations that create, receive, maintain or transmit PHI on behalf of a covered entity (e.g. many healthcare technology, billing and cloud providers). The HITECH Act (2009) made business associates directly liable for compliance with parts of HIPAA.

Key rules: the Privacy Rule, the Security Rule and the Breach Notification Rule.

Practical example: A US hospital (covered entity) and its cloud EHR hosting provider (business associate) are both directly liable under the HIPAA Security Rule for protecting ePHI.

Why this matters: Healthcare GRC experience is a strong differentiator; being able to explain HIPAA clearly also shows you can work with regulated health data in other countries.

Q: What is a Business Associate Agreement (BAA)?

Basic

A BAA is a contract required by HIPAA between a covered entity and a business associate (or between a business associate and its subcontractor). It sets out:

- Permitted uses and disclosures of PHI.
- Requirements to implement appropriate safeguards (Security Rule).
- Obligations to report breaches and security incidents.
- Flow-down obligations to subcontractors.
- Return or destruction of PHI at contract end.

Practical example: Before an AI transcription vendor processes clinicians' voice notes containing PHI, the hospital signs a BAA that requires safeguards, breach reporting and flow-down to its sub-processors.

Why this matters: No BAA, no PHI. It is a basic third-party control in any healthcare supply chain.

Q: What are the key principles of GDPR?

Basic

GDPR (EU General Data Protection Regulation, applicable since 25 May 2018) Article 5 sets out seven principles:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability — the controller must be able to demonstrate compliance.

GDPR also applies to organisations outside the EU that offer goods or services to, or monitor the behaviour of, people in the EU.

Practical example: Data minimisation: a fitness app asks only for date of birth (not full address) to calculate age-based heart-rate zones. Storage limitation: it deletes inactive accounts after 24 months.

Why this matters: These principles underpin most modern privacy laws, including GDPR and India's DPDP Act, so they transfer well between jurisdictions.

Q: What is PHI/ePHI under HIPAA, and what are the 18 identifiers about?

Basic

- Protected Health Information (PHI) is individually identifiable health information held or transmitted by a covered entity or business associate, in any form. ePHI is PHI in electronic form, which the Security Rule protects.
- It covers information about health condition, care provided or payment for care that identifies the person or could reasonably be used to identify them.
- The Safe Harbor de-identification method lists 18 identifiers (such as names, small geographic areas, dates other than year, phone numbers, email, medical record numbers, device identifiers, full-face photos) that must be removed, with no actual knowledge that the rest could identify someone.
- The alternative is Expert Determination by a qualified statistician.

Practical example: An analytics team wants to share appointment data with a research partner. Removing names, MRNs and exact dates but keeping year and state-level location helps meet Safe Harbor, so the data set can be shared as de-identified.

Why this matters: Knowing exactly what counts as PHI decides whether HIPAA applies to a data set, which is the first question in any healthcare privacy review.

Q: What is the HIPAA 'minimum necessary' standard?

Basic

- Covered entities and business associates must make reasonable efforts to use, disclose and request only the minimum PHI needed for the purpose.
- It applies to most uses and disclosures, but not to disclosures for treatment, to the individual, or where required by law, among other exceptions.
- In practice it is implemented through role-based access, data minimisation in reports and standard protocols for routine disclosures.

Practical example: A billing team's report originally included full clinical notes. Under minimum necessary, the report is changed to include only procedure codes, dates and amounts.

Why this matters: Minimum necessary is the HIPAA version of least privilege and data minimisation. Auditors and investigators often look for it after an incident.

Q: What rights do individuals have under GDPR?

Basic

- Right to be informed (transparency).
- Right of access (subject access request), usually answered within one month.
- Right to rectification.
- Right to erasure ('right to be forgotten'), with exceptions.
- Right to restriction of processing.

- Right to data portability.
- Right to object, including to direct marketing.
- Rights related to automated decision-making, including profiling (Article 22).

Practical example: A former patient of a private clinic in Germany asks for all her data. The DSAR process locates records in the EHR, CRM and email archive, applies legal exemptions where needed, and replies within the one-month deadline.

Why this matters: Handling data subject rights is a daily operational task for privacy teams, and failing to respond is a common basis for complaints.

Q: What is India's Digital Personal Data Protection (DPDP) Act 2023, and what are its key concepts?

Basic

The DPDP Act 2023 is India's general data protection law for digital personal data. The DPDP Rules were notified in November 2025, with most obligations phased in over the following months. Check the official timeline.

- Data Fiduciary (similar to a controller) and Data Processor; Significant Data Fiduciaries have extra duties such as a DPO, independent audits and DPIAs.
- Processing is based on consent (free, specific, informed, unambiguous, with clear notice) or certain 'legitimate uses' listed in the Act.
- **Data Principal rights:** access to information, correction and erasure, grievance redressal and nomination.
- **Duties:** reasonable security safeguards, breach notification to the Data Protection Board and affected individuals, and erasure when the purpose is served.
- Extra protections for children's data, and Consent Managers as a new type of registered intermediary.
- Enforcement by the Data Protection Board of India, with significant financial penalties.

Practical example: An Indian hospital-software company maps its GDPR programme to DPDP: it reuses its breach process and DSAR workflow, rewrites consent notices to DPDP standards (including language options), and assesses whether it might be designated a Significant Data Fiduciary.

Why this matters: Many GRC roles in India, and global companies with Indian operations or data, now need DPDP knowledge alongside GDPR.

Q: What are the safeguards in the HIPAA Security Rule?

Intermediate

The Security Rule protects electronic PHI (ePHI) through three categories of safeguards:

- **Administrative:** security management process (including risk analysis and risk management), assigned security responsibility, workforce security, training, incident procedures, contingency planning, evaluation and business associate agreements.
- **Physical:** facility access controls, workstation use and security, device and media controls.
- **Technical:** access control, audit controls, integrity, person or entity authentication, transmission security.

Implementation specifications are either 'required' or 'addressable'.

Practical example: Administrative: annual risk analysis and workforce training. Physical: badge access to the server room and workstation privacy screens. Technical: unique user IDs, audit logs and encryption of ePHI.

Why this matters: The required risk analysis is consistently highlighted in OCR enforcement — it is the foundation of HIPAA security compliance.

Q: What does 'addressable' mean in the HIPAA Security Rule?

Intermediate

'Addressable' does not mean optional. For each addressable implementation specification, the organisation must assess whether it is reasonable and appropriate in its environment and then:

- implement it, or
- implement an equivalent alternative measure, or
- not implement it if neither is reasonable and appropriate —

and in every case document the decision and rationale. Encryption of ePHI is a well-known addressable specification.

Practical example: Encryption at rest is addressable. A small clinic that decides not to encrypt a server must document why, e.g., the server is in a locked room and offline, and what equivalent measure it uses. 'Addressable' never means 'optional'.

Why this matters: Misunderstanding 'addressable' as optional is a common and costly compliance mistake.

Q: Summarise the HIPAA Breach Notification Rule.

Intermediate

When unsecured PHI is breached (unless a risk assessment shows a low probability that the PHI has been compromised):

- Affected individuals must be notified without unreasonable delay and no later than 60 calendar days after discovery.
- **Breaches affecting 500 or more individuals:** notify HHS within the same timeframe and, where more than 500 residents of a state or jurisdiction are affected, prominent media outlets.
- **Breaches affecting fewer than 500 individuals:** log them and report to HHS within 60 days of the end of the calendar year.
- Business associates must notify the covered entity of a breach.

PHI that is properly encrypted according to HHS guidance is not considered 'unsecured'.

Practical example: A stolen unencrypted laptop holds 1,200 patient records: notify individuals without unreasonable delay (no later than 60 days), notify HHS and prominent media because more than 500 residents of a state may be affected.

Why this matters: Incident response plans in healthcare must build in these timelines; GRC teams often own the breach risk assessment process.

Q: What are the GDPR lawful bases for processing, and what is the 72-hour rule?

Intermediate

Article 6 lawful bases:

- Consent.
- Contract.
- Legal obligation.
- Vital interests.
- Public task.
- Legitimate interests.

Special category data (e.g. health data) additionally needs an Article 9 condition.

The 72-hour rule (Article 33): a controller must notify the supervisory authority of a personal data breach without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is

unlikely to result in a risk to individuals. High-risk breaches must also be communicated to affected individuals. Processors must notify the controller without undue delay.

Practical example: A hospital processes health data for treatment using an Article 6 basis plus the Article 9(2)(h) healthcare condition. When a misdirected email exposes 40 patients' results on Friday afternoon, the DPO notifies the supervisory authority by Monday afternoon.

Why this matters: Breach timelines drive incident response design; lawful basis is the first question in any privacy review.

Q: What is the difference between a data controller and a data processor? What is a DPIA?

Intermediate

- **Controller:** decides why and how personal data is processed.
- **Processor:** processes personal data on behalf of and on the instructions of the controller (e.g. a SaaS or cloud provider). A written contract with required terms (GDPR Article 28) is needed.

A Data Protection Impact Assessment (DPIA, Article 35) is required before processing that is likely to result in a high risk to individuals — e.g. large-scale processing of special category data such as health data, or systematic monitoring. It describes the processing, assesses necessity and proportionality, identifies risks to individuals and the measures to address them.

Practical example: A hospital (controller) uses a cloud transcription service (processor) under an Article 28 contract. Before introducing AI-based patient triage, it runs a DPIA because the processing is large-scale special category data using new technology.

Why this matters: Roles determine obligations, and DPIAs are a privacy-by-design control that GRC teams often facilitate.

Q: How does a HIPAA risk analysis differ from a general risk assessment?

Intermediate

The HIPAA Security Rule requires an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of all ePHI the organisation creates, receives, maintains or transmits.

- **Scope must cover all ePHI, wherever it is:** EHR, imaging, email, laptops, backups, medical devices, cloud apps.
- It should identify threats and vulnerabilities, current controls, likelihood, impact and risk level, and be documented.
- It must be reviewed and updated periodically and after changes, and lead to a risk management plan.
- HHS enforcement actions frequently cite the lack of an accurate, enterprise-wide risk analysis.

Practical example: A clinic group's risk analysis covered only the EHR. Updating it to include imaging systems, a patient-messaging app and backup tapes finds that the tapes were unencrypted, which becomes a priority fix.

Why this matters: The risk analysis is the foundation of HIPAA Security Rule compliance, and its absence is one of the most cited issues in enforcement.

Q: What are the GDPR rules for international data transfers?

Intermediate

Chapter V of the GDPR restricts transfers of personal data to countries outside the EEA unless protection travels with the data:

- **Adequacy decisions:** the European Commission has recognised certain countries (and the EU-US Data Privacy Framework for certified US companies).
- **Appropriate safeguards:** Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs) and others.
- After the Schrems II judgment, exporters using SCCs should assess the destination's laws and practices (a transfer impact assessment) and add supplementary measures if needed.
- Limited derogations (such as explicit consent) apply for occasional, specific transfers.

Practical example: A European clinic uses a support team in India. It signs the EU SCCs with the vendor, performs a transfer impact assessment, and adds supplementary measures such as encryption and access logging.

Why this matters: Cloud and outsourcing almost always involve transfers. Getting the mechanism wrong is a common and costly compliance failure.

Q: What is a Record of Processing Activities (RoPA), and why is it useful beyond compliance?

Intermediate

Article 30 GDPR requires controllers and processors (with some exceptions) to keep a record of processing activities, including purposes, categories of data and data subjects, recipients, transfers, retention and security measures.

- It acts as the privacy equivalent of an asset inventory.
- It helps with DSARs (where is the data?), breach assessment (whose data is affected?), DPIA triggers and vendor management.
- It should be maintained by process owners with privacy oversight and reviewed regularly.

Practical example: When a marketing vendor reports a breach, the RoPA shows immediately that the vendor holds names and emails of 30,000 newsletter subscribers but no health data, so the risk assessment and notification decision take hours instead of days.

Why this matters: A current RoPA makes every other privacy process faster. Without it, organisations scramble during breaches and DSARs.

Q: An employee emails a spreadsheet with 300 patients' details to the wrong external address. Walk through your response.

Intermediate · Scenario

1. **Contain:** ask the recipient to delete it and confirm in writing, recall the message if possible, and preserve the details.
2. **Assess:** what data (identifiers, diagnoses?), how many people, who received it, and whether it was opened or forwarded.
3. **Apply the legal tests:** HIPAA's 4-factor risk assessment for a breach of unsecured PHI, GDPR Article 33 risk-to-individuals test, and any local law or contract.
4. Notify where required, within the deadlines (GDPR 72 hours to the authority, HIPAA without unreasonable delay and within 60 days), with legal involved.
5. Document everything, even if you conclude notification is not required.
6. **Fix the root cause:** email DLP rules, auto-complete clean-up, and training.

Practical example: The recipient, a clinic in another city, confirms deletion within an hour. The risk assessment finds a low probability of compromise, and this is documented. DLP now warns staff when a file with medical record numbers is sent outside the domain.

Why this matters: Misdirected email is one of the most common privacy incidents. A calm, documented process protects patients and the organisation.

Q: A US hospital wants to use a new cloud vendor for patient messaging, but the vendor will not sign a BAA. What do you advise?

Intermediate · Scenario

- Without a BAA, the hospital cannot let the vendor create, receive, maintain or transmit PHI on its behalf. Doing so would breach HIPAA.
- **Options:** find a vendor that will sign a BAA, use the vendor only for non-PHI messages (such as generic reminders with no health information), or negotiate.
- If the business still wants the vendor, document the decision and design controls so PHI cannot enter it.
- **Check the vendor's security anyway:** SOC 2 or ISO 27001, encryption and access controls.

Practical example: The vendor refuses a BAA, so the hospital selects a competitor that signs one and has a SOC 2 Type II. The original vendor is kept only for marketing newsletters, which contain no PHI.

Why this matters: This is a frequent real-world decision. The BAA is a legal precondition, not a negotiable nice-to-have.

Q: A data subject asks a company to delete all their data, but the company must keep invoices for tax law. What do you do?

Intermediate · Scenario

- Erasure is not absolute. Article 17(3) GDPR allows retention when needed to comply with a legal obligation.
- **Delete what is not needed:** marketing data, profiles, support chats beyond retention periods.
- Keep only the invoice data the law requires, restrict access to it, and delete it when the legal retention period ends.
- Reply to the person within the deadline explaining what was erased, what is retained, the legal reason and how long it will be kept.
- Record the request and the decision.

Practical example: The company deletes the customer's account, preferences and marketing history, keeps the invoices for the legally required period in a restricted finance archive, and sends a clear explanation within 3 weeks.

Why this matters: Balancing rights with legal obligations is the everyday reality of privacy work. Transparent responses prevent complaints.

Q: Your company processes Indian customers' data and the DPDP Rules are now notified. What do you do first?

Intermediate · Scenario

1. **Confirm applicability:** digital personal data processed in India, or outside India in connection with offering goods or services to people in India.
2. Build or update the data inventory and data flows, including processors and cross-border transfers.
3. Review notices and consent flows against DPDP requirements (clear, itemised notice, easy withdrawal, language options).
4. Set up processes for Data Principal rights, grievance handling and breach notification to the Data Protection Board and affected individuals.
5. Check retention and erasure rules, children's data handling and security safeguards.

6. Assess whether you may be a Significant Data Fiduciary, and plan against the phased compliance dates in the Rules.

Practical example: A health-tech firm headquartered outside India with Indian users runs a 6-week DPDP gap assessment, reuses its GDPR DSAR and breach processes, and rewrites its Indian consent screens in English and Hindi with a one-click withdrawal option.

Why this matters: A structured first response turns a new law into a manageable programme and shows leadership a clear plan and timeline.

Q: What did the January 2025 proposed HIPAA Security Rule update aim to change?

Advanced

In January 2025, HHS's Office for Civil Rights published a Notice of Proposed Rulemaking to update the HIPAA Security Rule. Main proposals included:

- Removing the distinction between 'required' and 'addressable' implementation specifications, making most of them required.
- Explicit requirements such as encryption of ePHI at rest and in transit, MFA, an asset inventory and network map, vulnerability scanning and penetration testing, and documented restoration capabilities.
- More specific requirements for business associates and for contingency planning.

A proposed rule is not final law. Check the current status before treating any of these as mandatory, and remember that many are already good practice.

Practical example: A health-tech vendor uses the proposed requirements as a gap checklist. MFA and encryption are already in place, but it lacks a documented network map and annual penetration test of a legacy system, so it funds both regardless of the final rule's timing.

Why this matters: Following the direction of regulatory change lets you plan ahead and explain the trend to leadership, while being careful not to overstate the legal status.

Q: How do you approach privacy for AI systems that process personal or health data?

Advanced

- **Lawful basis and purpose:** is training or using AI on this data compatible with the original purpose and the notice given to people?
- Do a DPIA (and where relevant an AI impact assessment) before deployment, covering bias, accuracy, explainability, security and automated decision-making rights.
- Minimise and de-identify data used for training, and control whether vendors may use your data to train their models.
- Ensure human oversight for decisions with significant effects on individuals.
- Address vendor terms (data location, retention, sub-processors) and security (prompt injection, data leakage).
- Keep records that let you answer regulators' and patients' questions.

Practical example: Before using an AI scribe in clinics, the hospital runs a DPIA, confirms that the vendor does not train on its data, stores recordings in-country, deletes audio after transcription, and requires clinicians to review every note.

Why this matters: AI multiplies existing privacy risks. Regulators in the EU, US, India and elsewhere are all applying existing privacy law to AI.

Q: Ransomware attackers claim they stole patient data from a business associate. What are your obligations as the covered entity?

Advanced · Scenario

- Activate incident response and legal counsel. Get facts from the business associate quickly: what systems, what data, which patients, what timeline.
- Under HIPAA, the business associate must notify the covered entity of a breach. The covered entity is generally responsible for notifying individuals, HHS and, where 500+ residents of a state are affected, the media, unless the BAA delegates this.
- HHS guidance treats ransomware encryption of PHI as a presumed breach unless a low probability of compromise can be shown.
- Check other laws that apply (state laws, GDPR, local rules) and contract duties to customers.
- Review the BAA and the vendor's controls afterwards, and decide whether to continue the relationship.

Practical example: A transcription vendor confirms data on 8,000 patients was stolen. The hospital's breach team coordinates notification letters through the vendor (as agreed in the BAA), reports to HHS, notifies media where required, and adds stronger security terms to the contract.

Why this matters: Third-party breaches are common in healthcare, and responsibility for notification often stays with the covered entity even when the vendor was at fault.

Q: A marketing team wants to use patient lists for a new wellness campaign. What privacy questions do you raise?

Advanced · Scenario

- Under HIPAA, most marketing communications using PHI need the patient's written authorisation. There are limited exceptions, such as face-to-face communications.
- Under GDPR or the DPDP Act, check the lawful basis (often consent for marketing), the original purpose and the notice given.
- Health data is special category or sensitive, which requires higher standards.
- Check opt-outs, electronic marketing rules and whether third-party tools (email platforms, ad pixels) would receive health information.
- Recommend an approach based on opt-in consent, collected separately from treatment consent.

Practical example: Instead of using the patient list, the team launches an opt-in wellness newsletter on the website and in clinics. Ad-tracking pixels are removed from patient portal pages after a privacy review.

Why this matters: Marketing use of health data has led to major regulatory actions, especially around tracking pixels and sharing with ad platforms.