FDPPI
Think Data, Think FDPPI
Foundation of Data Protection Professionals in India
(Section 8 Company, Not for Profit, Limited by Guarantees)
CIN Number: U72501KA2018NPL116325:
GSTN: 29AADCF4963H1ZC
www.fdppi.in: E Mail: fdppi@fdppi.in : Ph: 8310314516

DGPSI-Hospital

DGPSI stands for Digital Governance and Protection Standard of India. It was developed by Naavi and FDPPI for compliance of DPDPA. Most recently an extension of the framework was created for DGPSI-GDPR. Otherwise the family of DGPSI today includes the following frameworks all focussed on DPDPA Compliance.

1.DGPSI-Full Version:

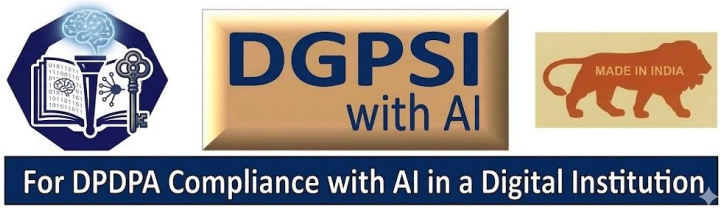
Consists of 50 model implementation specifications built on 12 foundation principles. Was the first framework developed and includes concepts like Data Valuation, Distributed Responsibility, Process based compliance, DPDPA oriented Data Classification, DTS as measure of maturity of implementation, Hybrid entity concept for identifying the organization as a combination of (SDF Process+DF Process+DP process) etc. When this was published on 24th 2023. This framework was meant to comply with DPDPA along with ITA 2000 and Data Governance principles related to personal data protection released as a Draft by BIS in August 2023.

2.DGPSI-Lite:

Simultaneously with the release of DGPSI-Full version, a lighter version called DGPSI-Lite was released for the benefit of SMEs. This version contained 36 implementation specifications. This focussed only on the legal compliance of DPDPA.

3. DGPSI-AI

In July 2024, prior to the IDPS event, Naavi/FDPPI released the framework DGPSI-AI to guide the Data Fiduciaries using AI tools for processing personal data. This also contained 6 principles and 9 implementation specifications which were considered additional to the 12 principles and 50 implementation specifications of DGPSI-FULL. Currently we refer this version as “DGPSI- with AI”



4. DGPSI HR

Subsequently in December 2025-January 2026, based on the experience with Manufacturing companies where the DPDPA Risk was mostly concerned with the HR divisions, a special framework for HR operations was developed and termed DGPSI-HR. This included AI aspects also. This has now been developed as a 30 specification version with the inclusion of POSH, ITA 2000 and RTI (for public authorities) besides AI.

5. DGPSI-DP

Along with DGPSI-HR, Naavi/FDPPI also released a "Best Practice Framework" for Data Processors named DGPSI-DP. Though Data Processors are not legally mandated to be compliant with DPDPA, considering the impact of Section 72A of ITA 2000 and the contractual bindings mandated under DPDPA for Data Fiduciaries, DGPSI-DP was recommended for Data Processors. This contains 36 implementation specifications including AI and gives primacy to the Contract with the Data Fiduciary.

6. DGPSI-GDPR

Around December 2025-January 2026 itself , DGPSI was also extended for GDPR implementation so that Indian companies which have a stack of GDPR related personal data along with DPDPA could be serviced by the DPDPA auditors.

Despite these frameworks, it was found that specific sectors like Hospitals, Banks and Educational Institutions were finding it difficult to comply with DPDPA which was a law common for all sectors and organizations of all sizes.

Hence it was necessary to consider specific versions of DGPSI applicable to Hospitals, Banks and Educational Institutions.

Some special aspects that needed consideration for the Hospital was that "Data" in a hospital system could represent "Life" which was much more valuable than the "Data Valuation Concept" pioneered under the DGPSI-Full version.

There was a felt need to ensure that NABH accreditation principles of "Patient Safety" had to be integrated into the principles of "Personal Data Protection" in the DPDPA. This

was required at all stages of personal data management from "Establishing the Legal Basis", "Maintaining Security", "Managing the Data Breach Situation".

It was felt that in a "Data is Life" situation, the concepts of Information Security embedded in DPDPA itself need a change. Similarly, under DPDPA, since Data is life, every hospital which deals with patient data was considered as "Significant Data Fiduciary". Hence every hospital had to integrate the CISO's role and DPO's role along with the "Patient Safety officer" (PSO)'s role and come up with a "Personal Data Protection Model" which was consistent with both the CISO's approach based on CIA and the PSO's approach of "Safe health care outcome". The PSO's objective was protection of the health care activity of the hospital and data protection and privacy rights protection were subordinate to the objective of maintaining the patient safety.

This key aspect has been included in the DGPSI-Hospital framework which is contained in this note.

Similarly, the DGPSI-Bank also have some unique requirements which need to be integrated with RBI guidelines such as Data Localization, "Nomination of Money in the account distinct from Nomination of Data", "Model based regulation of AI", "Presence of Section 70 notified systems" etc. The DGPSI-Education will also have its own uniqueness in the form of the hierarchy of the University, College and individual departments with different degrees of autonomy. These will be addressed when the frameworks for Banks and Educational Institutions are finalized.

The framework will be structured on the basis of DGPSI-Full version along with DGPSI-AI consisting of 18 Foundation Principles and 59 implementation specifications for the Hospital as a Data Fiduciary. (If Hospital is involved in AI development), the development unit would be considered as a different "Data Processor or joint Data Fiduciary" and compliance will be worked accordingly.

In the responsibility centers, DGPSI-Full now identifies 5 units namely the Top Management, DPO, HR, Legal and IT. In the Hospital context the DPO role will be integrated with a team of three persons namely the CISO, DPO and PSO. This team called CDP triumvirate will provide oversight to the implementation of DPDPA along with ITA 2000 and PSO obligations simultaneously. Externally each of the triumvirate will face their respective regulators while internally they act as a team under the guidance of the Apex DPDPA Governance Committee headed by an Independent Director.

The PSO may pursue a separate NABH accreditation framework and CISO can pursue a separate ISMS framework for their respective functions while DGPSI-Hospital will be the framework for DPDPA compliance.

The DGPSI-Hospital framework may be further fine tuned for DGPSI-Diagnostic Centers where NABL accreditation may be required.

No MIS-H	Description of Specifications	LRL
	Management Responsibilities	
1	Considering the Risk to human life arising in the operations of a hospital, every hospital shall consider itself as a "Significant Data Fiduciary" and devise its policies accordingly. In case the Hospital is using AI, a special care is taken to ensure that the unknown risks arising out of AI usage does not materially affect the responsibilities of the hospital. Organization shall designate a DPO with necessary credentials and provide support in terms of people, budget and technology and external consultancy. Organization shall also designate an AI regulation officer (AIRO) who will be responsible for ensuring that the use of AI in different processes does not materially affect the health care functions of the hospital. AIRO will work closely with the DPO, PSO and CISO to ensure that their responsibilities are not adversely affected by the use of AI both by the organization and its vendors/associates. Organization shall also form a three member Compliance team consisting of the DPO, CISO and the PSO to continuously supervise and be responsible for compliance of DPDPA, ITA 2000 and NABH accreditation as may be required. Each of them will externally face their respective regulators independently while coordinating their activities internally for a common goal of Patient Safety. In the case of a public authority, organization will take note of the exemption availability if any. However the CPIO (under RTI obligations) will work independently but in close consultation with DPO. Organization shall establish appropriate policies to ensure harmonious functioning of the DPO, CISO, PSO and CPIO (where applicable) to ensure that the regulatory requirements under different statutes are respected and managed effectively.	

2	Organization shall constitute the Data Governance and Data Protection committee under the chairmanship of a Board member, preferably an independent director, Designated DPO/Compliance officer as the Secretary and representation of key stakeholders such as the CEO, CFO, CMO, CTO, CISO, Chiefs of Legal, HR. The PSO shall be part of the Committee.	
3	Organization shall appoint an External Independent Data Auditor with necessary Credentials	
4	Organization shall identify every purpose for which personal data is being used in digital form and recognize a "Process" associated with the purpose and create an inventory. AI processes will be also considered as an independent process . Each such process will have a specific process owner who will be responsible for compliance within the process. Each process will be managed as a separate unit with exclusive DPDPA requirements such as data minimisation, retention requirements, access requirements etc which will be integrated with the enterprise policies. Data recognized by each process owner as being used will be used for creating a consolidated data inventory with appropriate classifications. The organizational oversight of each process will be appropriately tailored based on the sensitivity of the process. Processes using Personal data to which DPDPA is applicable (DPDPA Protected Data or DPD) are properly segregated from other personal data and non personal data processes.	
5	Organization will cause conduct of a DPDPA Risk assessment and develop a document that defines the scope of the DPDPA compliance implementation program from an independent data auditor.	
6	Organization shall ensure that all employees, consultants and vendors are provided appropriate awareness of the legal provisions of the Act. The "Awareness" needs to be supplemented with "Acceptance" through appropriate ethical assurance and cover all employees, consultants and vendors exposed to personal data of the organization.	
7	Organization shall create an "Exception" policy to establish an appropriate exception handling systems with adequate checks and balances with appropriate documentation so that Business Continuity and Patient Safety is not compromised.	
8	Organization shall establish an appropriate policy to recognize the financial value of data and assign a notional	

	financial value to each data set and bring appropriate visibility to the value of personal data assets managed by the organization to the relevant stakeholders. However the financial value of the data shall not override the value of data as a representation of human life and appropriate steps will be taken to ensure that data monetization shall be strictly regulated.	
9	Organization shall establish an appropriate policy for identifying and factoring the impact of data protection laws at all levels of business operations commencing from marketing of new business and through the data processing lifecycle.	
10	The organization shall establish appropriate policy for using services of third-party contractors for data processing and enter appropriate enforceable contractual agreement with appropriate assurances towards data protection. Such contracts shall also enable audits and indemnities as may be required and cover all services related to personal data processing including manpower outsourcing, cloud services, shared services for hosting of website, e-mail, application development etc. Such contractual arrangements shall cover sharing of personal data for research or under any societal obligations. All contract employees, consultants, and outsourced personnel engaged by the Organization who have access to or process Personal Data shall act under the authority of the Organization and shall be bound by written confidentiality, security and data- protection obligations aligned to the Digital Personal Data Protection Act, 2023. Where a consultant or service provider independently or jointly determines the purposes and means of processing Personal Data, such party shall be treated respectively as a Data Fiduciary or Joint Data Fiduciary for that processing	
11	Organization shall establish a system for monitoring and managing the relations with regulatory agencies such as DPB, CERT IN and other sectoral and jurisdictional regulators.	
12	Organization shall establish appropriate policies to ensure that sharing of personal data by any of the employees and consultants shall be strictly on need to know basis subject to data minimisation requirements and Non Disclosure agreements.	
13	Organization shall establish an appropriate policy for maintaining digital presence on the web, mobile, Wearables, IoT etc with adequate security against misuse of applicable	

	data protection laws including intellectual property and cyber crime laws.	
14	Organization shall establish a suitable system for monitoring any devices which process personal data and provide automated outputs to ensure integrity of the outputs.	
15	Organization shall develop and implement an appropriate "AI Usage Policy" covering all software algorithms and models whether developed in house or outside, whether they are supported by generative AI or Agentic AI or otherwise to ensure AI risk mitigation and availability of human handlers for every AI process.	
DPO Responsibilities		
16	Organization shall establish data processing policies for each process where personal data to which DPDPA is applicable (DPD) is processed, covering the necessity of the process, the requirements, the notice , the legal basis and any other relevant information. Principles of Purpose limitation, Data Minimization, Data Retention minimization, Data accuracy, Data Access on need to know basis are incorporated in each of the policies to which the Process owner shall be accountable. There shall be no processing that is not covered either by exemption or legitimate use or specific consent. The process owners (external data processors) shall be made responsible for the compliance of DPDPA for the process and necessary commitments shall be on record.	
17	Organization shall establish an appropriate policy for continuing use of legacy personal data and for continuing use of personal data after the end of the purpose for which it was collected. Such policy shall include sending of notice, monitoring and documenting the response and initiating necessary follow up actions. Where continued processing is not justified, committing the data to an anonymized archival or destruction shall be considered. Where continuation of processing is justified under legitimate basis, appropriate secured archival are created to ensure elevated security for processing such data in the absence of appropriate consents.	
18	Organization shall establish policies for processing DPD under a valid consent.	

	Such policy shall include sending of notice for each process, monitoring and documenting the response and initiating necessary follow up actions. Separate policies for different channels of interaction with data principals such as Web or Mobile shall be established. All consents and any modifications thereof shall be adequately authenticated and preserved with a unique tracking ID for such period as is required under law.	
19	Organization shall establish an appropriate policy for managing relationship with Consent Managers including setting up technical measures for receiving and withdrawing consent or for exercising any rights of the data principal.	
20	Organization shall establish an appropriate policy for handling unstructured personal data including discovery, merging with other structured collection of personal data, erasure in unstructured form etc.	
21	Organization shall establish an appropriate policy for providing "Data Access" rights to data principals including verifiable identification along with the Right to Correction, Withdrawal of consent and Deletion. The requirement shall be consistent with the requirements for compliance of ITA 2000 and Patient Safety regulations.	
22	Organization shall establish an appropriate policy for incident management in the context of Privacy with relevant incident identification, incident validation and incident management. Such policy shall be consistent with the requirements of the PSO and CISO for NABH and ITA 2000 purposes.	
23	Organization shall establish an appropriate policy for data breach notification for timely recognition and notification to all stakeholders under data protection laws, other laws such as ITA 2000 or NABH or any other sectoral regulations or the law enforcement authorities as may be required. The policy shall include immediate measures to be undertaken for prevention, and detection of privacy incidents and corrective measures.	
24	Organization shall adopt an appropriate policy for disclosure and destruction of personal data as per all applicable laws.	
25	The Organization shall establish an appropriate policy for implementing security measures at different levels such as Physical, logical, application or data level access required to protect unauthorized access to personal data assets whether they are located in the organizational resources or with data processors or cloud operators or employees.	

26	The Organization shall establish an appropriate policy for acquisition or disposal or sharing or licensing of hardware and software assets from reliable and verified sources with assurance on security.	
27	The Organization shall establish an appropriate policy for documentation of all compliance activities	
28	The organization shall establish appropriate internal audit measures and facilitate external audit where required. In the case of AI, DPIA is supported by annual external data auditor's evaluation at least once a year.	
	Legal Responsibilities	
29	The organization shall establish appropriate policies for Grievance redressal both under DPDPA as well as ITA 2000 and NABH regulations.	
30	Organization shall establish an appropriate policy for providing "Nomination" facility to data principals including verifiable identification of the nominee and description of the data assets to which nomination is applicable.	
31	Organization shall establish an appropriate policy for collection and verification of status of a minor or other disabled data principals who are represented by legal guardians and to manage such consent along with restrictions such as behaviour monitoring or targeted advertising as well as transmission of consent control back to the minor/disabled person on termination of the power of the guardian.	
32	Organization shall establish an appropriate policy for structuring contracts with business associates as instruments of ensuring compliance. Such policy shall ensure updating for data protection requirements, identifying inter-se responsibilities, contact persons, expiry etc.	
33	Organization shall establish an appropriate policy for structuring contracts with vendors of medical equipments where personal data is processed.	
34	Organization shall establish appropriate policies for structuring contracts with Consulting Doctors, external diagnostic centres, external medical service providers including food and other supplies to ensure compliance of DPDPA.	

	HR Responsibilities	
35	Organization shall maintain an inventory of employees with relevant policy for assigning responsibility under distributed responsibility, providing privacy awareness training on a periodical basis.	
36	Organization shall establish an appropriate Privacy policy for processing personal data of employees, including those who are in the recruitment process or have ceased to be employees, or working on manpower supply contracts, as per applicable laws. Separate privacy policies may be executed with consultant doctors or those with whom DPD is shared for legitimate purpose or on consent basis.	
37	Organization shall establish an appropriate augmented HR Policy for developing a Compliance Culture in the organization including imposition of duties, sanctions and incentives.	
38	Organization shall establish a whistleblower policy covering employees and extending to external participants including the public with appropriate witness protection and incentives.	
39	Organization shall establish an appropriate accepted usage policy of resources allocated by the organization including in the context of working from locations outside the office and using Own Devices with relevant sanctions for violation.	
	Technology Responsibilities	
40	Organization shall develop an Inventory of Processes, which generate, Use, Disclose or Destroy Personal Data with unique process ID assigned to each process and tagging the purpose of processing. Each process shall also identify and tag the contextual role of the organization as Data Fiduciary, Data Processor or Joint Data Fiduciary. Each Process shall identify a process owner who shall as an Internal Data Controller be responsible for compliance within his area of operation. Each process shall identify the input output data, nature of processing, storage status and movement of data during processing and storage. Each process shall adopt dynamic access permissions on a need to know basis. Each process shall tag the restrictions on the rights of use as per contractual permissions covering data protection laws, IPR laws, sectoral regulations etc.	

41	Organization shall create an inventory of personal data as a data set with a unique Master Data Management (MDM) with necessary attributes. The attributes shall include the source of the data and the legal basis of collection. Each personal data set shall be associated with classification attributes such as Minor, Employee, Sensitive, applicable jurisdiction etc. Organization shall establish a technology architecture that creates an inventory of personal Data Identifiers, and run continuous search for periodical updating, merger, de-duplication, and classification of data as personal data as combinations of data identifiers. Organization shall identify a unique ID as a Core ID associated with the MDM ID and establish a system for populating other personal data attributes on an ongoing basis	
42	The Organization shall set up an appropriate policy for use of Pseudonymization, anonymization and data masking for secure disclosure of personal data between processes or for disclosure.	
43	The organization shall create a Centralized Personal Data Store and secure remote access architecture with virtual processing.	
44	The Organization shall establish an appropriate set of information security controls necessary for protecting the data prevention of unauthorized access, modification or denial of access applicable to personal data and also data leakage and data exfiltration along with Shall include policy for using encryption in storage, transit, processing along with required key management system. Shall include data integrity management and non-repudiable authentication of data with the use of appropriate techno legal tools. Shall also include system updating and malware etc.	
45	The Organization shall establish an appropriate policy for handling transit of data across jurisdictional borders as per applicable law including sectoral laws	
46	The Organization shall establish an appropriate policy for disaster recovery and Business Continuity to meet requirements during exigencies. Shall include escrow of encryption keys, critical software code etc. where appropriate.	
47	The Organization shall establish an appropriate policy for adopting technical measures to segregate processing of	

	personal data of different jurisdictions and to maintain arm's length relationship between service units belonging to different jurisdictions.	
48	Organization shall collect an authenticated "Explainability" document from the developer as part of the licensing contract indicating the manner in which the AI functions in the processing of personal data and the likely harm it may cause to the data principals.	
49	Organization shall collect a document an assurance from the licensor that 1. The AI software is adequately tested at their end for vulnerabilities, preferably from the third party auditor. The document should state that the "When deployed for data processing, the AI Software is reasonably secured against vulnerabilities that may adversely affect the confidentiality, integrity and availability of data and the Privacy principles where the data processed is "Personally identifiable data". 2. Sufficient guard rails exist to protect the Data Principals whose data may be processed by the deployer.	
50	The Deployer of an AI shall take all such measures that are essential to ensure that the AI does not harm the society at large. In particular the following documentation of assurances from the licensor is recommended. 1.The AI comes with a tamper-proof Kill switch. 2.In the case of Humanoid Robots and industrial robots, the Kill Switch shall be controlled separately from the intelligence imparted to the device so that the device intelligence cannot take over the operation of the Kill Switch. 3.Where the kill switch is attempted to be accessed by the device without human intervention, a self destruction instruction shall be built in. 4.Cyborgs and Sentient algorithms are a risk to the society and shall be classified as Critical risks and regulated more strictly than other AI, through an express approval at the highest management level in the data fiduciary. 5.Data used for learning and modification of future decisions of the AI shall be imparted a time sensitive weightage with a "Fading memory" parameter assigned to the age of the observation. 6. Ensure that there are sufficient disclosures to the data principals about the AI risk	