



# ***CUSTODIAL KEYS, CONSENTING PRINCIPALS, Locating Agency and Data-Fiduciary Liability in Blockchain-Based Health Data Architectures under the Digital Personal Data Protection Act, 2023***

***Ankul Prajapati<sup>1</sup>, Astha Chauhan<sup>2</sup>, Karan Gangrade<sup>3</sup>***

Name of Institution: National Law Institute University, Bhopal

## **ABSTRACT :**

Blockchain-based health data architectures promise that the patient, rather than the hospital, the insurer or the state, holds the cryptographic key to her own medical history. Key loss, however, is irreversible, and for a population-scale system in India it makes custodial or semi-custodial key management a practical necessity. This paper asks in what legal capacity a custodial key-holder acts when it signs consent grants and withdrawals on a patient's instruction, and whether holding that key and executing transactions on her behalf makes the custodian a Data Fiduciary under Section 2(i) of the Digital Personal Data Protection Act, 2023. It adopts a doctrinal method, reading the Act and the Digital Personal Data Protection Rules, 2025, the Indian law of agency and trusts, Supreme Court decisions on privacy and medical confidentiality, Ayushman Bharat Digital Mission documents, and European and international guidance on blockchain roles and crypto-asset custody against a technical account of how consent and revocation operate on a ledger. The paper argues that an instruction-following custodian is ordinarily the patient's agent, and that possession of the key does not by itself confer fiduciary status; status attaches, function by function, where the custodian exercises autonomous discretion over the terms of processing. It proposes a three-part framework comprising an instruction-fidelity test, a discretion-locus test and a registration-convergence rule, under which a custodian whose discretionary functions replicate the statutory role of a Consent Manager is treated as performing that role. It concludes with recommendations for the Data Protection Board, the Ministry of Electronics and Information Technology, the National Health Authority and system designers. Because the Act and the Rules commence in phases, with Consent Manager registration from 13 November 2026 and the main obligations from 13 May 2027, the analysis is prospective.

**Keywords,** Data Fiduciary; Custodial Wallets; Consent Manager; Blockchain; Health Data

## **I. INTRODUCTION**

Blockchain-based health data architectures can be defended on a single normative promise, that the patient, and not the hospital, the insurer, or the state, should hold the keys to her own medical history. Cryptographic self-sovereignty is presented as the technical instantiation of the informational autonomy that K.S. Puttaswamy onward, has increasingly recognised as a facet of the right to life and personal liberty under Article 21.<sup>1</sup> The Supreme Court recognised that medical information falls within an individual's zone of privacy and that disclosure of such information may, in appropriate circumstances, infringe the patient's right to privacy, although that right may yield where disclosure is justified by a competing public interest in *Mr. 'X' v Hospital 'Z'*. The subsequent Aadhaar judgment further developed the constitutional understanding of informational privacy, recognising that individuals have an interest in controlling the collection, storage and dissemination of personal information, thereby strengthening the constitutional foundation for treating control over health data as an aspect of individual autonomy.<sup>2</sup> The architecture includes a private cryptographic key, generated and held exclusively by the data principal, which becomes the sole instrument through which access to her health records can be granted, reviewed, or withdrawn. No hospital administrator, no government database operator, and no third-party processor need ever hold that key. Consent, on this account, ceases to be a form filled out once at intake and instead becomes a live, continuously exercisable cryptographic capability.

This, however, rests on an empirical assumption that fails for the overwhelming majority of prospective users of any population-scale health data system in India, that ordinary patients are willing and able to generate, secure, back up, and correctly use a private cryptographic key. The assumption fails not merely for reasons of transient digital illiteracy but for structural reasons intrinsic to key-based cryptography itself. A lost private key is not recoverable

<sup>1</sup>Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1; Constitution of India 1950, art 21.

<sup>2</sup>Mr 'X' v Hospital 'Z' (1998) 8 SCC 296, clarified in Mr 'X' v Hospital 'Z' (2003) 1 SCC 500; Justice KS Puttaswamy (Retd) v Union of India (2019) 1 SCC 1 (Aadhaar).

through any password-reset mechanism, because the entire design of asymmetric cryptography dispenses with the central authority that a password-reset function presupposes. For a banking application, key loss is inconvenient. For a health record containing the only accessible copy of an oncology history, an allergy profile, or a decade of chronic-condition data, key loss is catastrophic and irreversible. Designers of real-world health-data systems therefore converge, almost without exception, on custodial or semi-custodial key management, a wallet application, hospital network, or platform operator generates and stores the private key on the patient's behalf, and the patient interacts with the system through conventional, recoverable credentials such as a password, a one-time password, or a biometric prompt.

The difficulty is that custodial key management reintroduces, through the back door, precisely the centralised intermediary that the blockchain architecture was designed to eliminate. If the patient does not herself hold the key that alone can execute a consent grant or a consent withdrawal on the underlying ledger, then someone else does. That someone else becomes, as a matter of brute technical fact, the only party capable of giving cryptographic effect to the patient's statutory rights, notably the right to withdraw consent under Section 6(4) and the rights of access, correction and erasure, grievance redress, and nomination under Sections 11 to 14 of the Digital Personal Data Protection Act, 2023.<sup>3</sup>

---

## RESEARCH PROBLEM

This paper asks two connected doctrinal questions that arise from that fact. First, in what legal capacity does the custodial key-holder act when it signs a transaction on the patient's instruction, is it an agent within the meaning of the Indian Contract Act, 1872, a bailee, a trustee, or something the existing private-law taxonomy does not neatly capture? Second, does the act of holding custody over the patient's signing key, and executing transactions on her behalf, itself satisfy the statutory definition of a Data Fiduciary under Section 2(i) of the DPDP Act, such that the wallet or platform operator acquires the full suite of fiduciary obligations under Chapter II of the Act, independent of and in addition to the obligations already borne by the hospital or health information provider whose records are being accessed.

The analysis proceeds by first explaining, in some technical detail, how key-based consent and revocation actually function at the protocol level, because the legal characterisation offered here depends on a precise understanding of what a custodian does when it signs on a patient's behalf. It then maps that technical reality onto the DPDP Act's consent architecture, onto the law of agency, and onto the statutory test for fiduciary status, before turning to the Ayushman Bharat Digital Mission as an illustrative, though not yet blockchain-native, setting in which this question will have to be answered in practice. The paper's central claim is that custodial key-holding does not automatically make an entity a Data Fiduciary, but that it does so wherever the custodian exercises any autonomous discretion over the terms of processing beyond the bare execution of the patient's instructions, and that Indian data protection law currently lacks an explicit doctrinal vocabulary for identifying that threshold. Because the Act and the Rules commence in phases, that claim is prospective, and Section VIII sets out the timetable on which it will become operative.

---

## II. RESEARCH OBJECTIVES

This paper pursues four objectives,

1. To explain, at the level of the ledger, how key-based consent and revocation operate, and why that mechanism makes custodial or semi-custodial key management the structurally dominant arrangement for any population-scale health-data system in India.
2. To determine the private-law capacity in which a custodial key-holder acts when it signs transactions on a patient's instruction, by testing the relationship against the law of agency, bailment, and trusteeship.
3. To test whether custodial key-holding satisfies the statutory definition of a Data Fiduciary under Section 2(i) of the Digital Personal Data Protection Act, 2023, and to identify the point at which a custodian moves from executing a patient's determinations to determining the purpose and means of processing itself.
4. To propose a workable liability framework, together with concrete recommendations for the Data Protection Board, the Ministry of Electronics and Information Technology, the National Health Authority, and system designers, that accounts for the overlap between custodial key-holding and the registered Consent Manager category.

---

## III. RESEARCH QUESTIONS

The Research Problem set out in Part I poses two doctrinal questions, and a third follows from them.

---

<sup>3</sup>Digital Personal Data Protection Act 2023, s 6(4) and ss 11-14.

1. In what legal capacity does the custodial key-holder act when it signs a transaction on the patient's instruction is it an agent within the meaning of the Indian Contract Act, 1872, a bailee, a trustee, or something the existing private-law taxonomy does not neatly capture?
2. Does the act of holding custody over the patient's signing key, and executing transactions on her behalf, itself satisfy the statutory definition of a Data Fiduciary under Section 2(i) of the Digital Personal Data Protection Act, 2023?
3. Where a custodian's discretionary functions substantially replicate the statutory role of giving, managing, reviewing, or withdrawing consent on a data principal's behalf, should that custodian be treated as performing the function of a Consent Manager, and be required to satisfy the registration and operational conditions that Rule 4 of the Digital Personal Data Protection Rules, 2025 imposes?

---

#### IV. RESEARCH METHODOLOGY

This paper adopts a doctrinal method. Its primary sources are the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, including the First Schedule to the Rules; the Indian Contract Act, 1872 and the Indian Trusts Act, 1882; decisions of the Supreme Court of India on privacy and medical confidentiality; and official documents of the National Health Authority relating to the Ayushman Bharat Digital Mission. The comparative component is confined to two reference points, the controller-processor distinction under the General Data Protection Regulation, as applied to blockchain networks in guidance of the Commission Nationale de l'Informatique et des Libertés and the European Data Protection Board, and the duties that financial regulation imposes on custodians of crypto-asset private keys. The comparison is functional rather than exhaustive, and is used to test the paper's analytical categories, not to import foreign rules.

The technical description of key custody in Sections V to VII is a descriptive account of how public-key cryptography, custodial and threshold key management, and ledger-level consent and revocation operate in permissioned and public blockchains. It rests on standard accounts of those technologies, and its blockchain-specific premises, namely immutability, confirmation latency, and the treatment of keys and wallet addresses, are consistent with the technical description in the European Data Protection Board's Guidelines 02/2025. It is offered as the factual premise for the legal analysis and not as an independent technical study, and no empirical fieldwork was undertaken. The Act and the Rules are only partly in force, so the analysis of Chapter II duties is prospective; Section VIII sets out the commencement timetable on which that analysis depends.

---

#### V. PUBLIC-KEY CRYPTOGRAPHY AND THE ARCHITECTURE OF ON-CHAIN IDENTITY

A coherent legal analysis of key custody has to begin with what a cryptographic key actually is and does, because the law's ordinary intuitions about possession and control map onto this technology only imperfectly. Every account or identity on a blockchain network is defined by a mathematically linked pair of numbers, a private key, which must never be disclosed, and a public key, which is derived from the private key through a one-way function and can be shared freely. The public key, or an address derived from it through hashing, functions as the visible identifier on the ledger, comparable to an account number. The private key functions as the sole instrument of authorisation, any transaction, whether it transfers value, grants access, or records a consent artefact, must be digitally signed using the private key before the network will treat it as valid. The signature can be verified by any participant using only the public key, without that participant ever learning the private key itself. This is the cryptographic property that makes decentralised verification possible at all.

The critical point for present purposes is that a blockchain protocol has no independent means of knowing who, in the offline world, controls a given private key. The protocol recognises only cryptographic control. Whoever can produce a valid signature is treated, for every purpose internal to the system, as the legitimate holder of that address and everything associated with it. This is sometimes summarised in the crypto-industry maxim that possession of the key is possession of the asset, and the maxim is not merely colloquial; it describes the actual logic of the consensus protocol. Real-world identity is bound to a blockchain address only through an external, off-chain linkage, such as a know-your-customer registration process, a government-issued digital identity like the Ayushman Bharat Health Account number, or an enrolment process run by a hospital network. The blockchain itself is indifferent to whether the entity signing a transaction is the patient, her nephew, a call-centre operator, or an automated script running on a cloud server, provided that entity holds the corresponding private key.

This indifference is not a defect to be engineered away; it is the foundational design choice that gives blockchain systems their tamper-resistance and their independence from any single trusted authority. But it has a direct legal consequence that is often elided in enthusiastic accounts of blockchain-based patient empowerment. The statement that a patient controls her own health data because the architecture is built on patient-held keys is true only to the extent that the patient actually, physically, and continuously controls the private key. The moment that control is delegated, even partially, to a wallet provider, an app operator, or a hospital-run key management service, the cryptographic guarantee of patient control becomes, in substance, a guarantee of custodian control exercised nominally on the patient's behalf. Whether that nominal exercise is legally sufficient to preserve the patient's

rights under the DPDP Act is precisely the question this paper investigates, and it cannot be answered without first taking seriously the mechanics just described.

---

## VI. CUSTODIAL AND NON-CUSTODIAL KEY MANAGEMENT, A FUNCTIONAL TAXONOMY

Real-world key management systems fall along a spectrum rather than into a strict binary, and the position of a given health-data wallet on that spectrum determines the legal analysis that follows. At one end sits pure non-custodial management, in which the patient generates her own key pair, typically through a hardware device or a secure enclave on her own smartphone, and no external party ever has access to the private key in usable form. The patient authorises every transaction directly, and the wallet software merely constructs the transaction and passes it to the device for signing. This model best realises the self-sovereignty promise, but it imposes the full weight of key security on an individual who may have no experience with cryptographic key management, and it offers no recovery path if the device is lost, stolen, or damaged, which for a rural patient without a stable digital footprint is a realistic and frequent occurrence.

At the other end sits full custodial management, in which a wallet provider, a health-technology company, or a hospital consortium generates the key pair on its own infrastructure, typically within a hardware security module or an encrypted server-side vault, and the private key never leaves that infrastructure. The patient authenticates to the provider's application using ordinary, recoverable credentials, and the provider's backend signs transactions on the patient's instruction, communicated through the application's user interface or, in lower-connectivity settings, through an agent-assisted or call-centre channel. This model trades cryptographic self-sovereignty for usability and recoverability, and it is, as a matter of observed practice across every major consumer-facing crypto-asset platform globally, the dominant model wherever a service is aimed at a mass, non-technical user base rather than a specialist or institutional one.

Between these two poles sit a range of semi-custodial or shared-custody architectures, of which threshold or multi-party computation signing schemes are the most significant for health-data design. In a typical implementation, the private key material is never assembled in a single location at all; instead, it is mathematically sharded, so that a valid signature requires cooperation between a fragment held on the patient's own device and a fragment held on the provider's servers, with neither fragment alone sufficient to authorise a transaction. This architecture is attractive precisely because it avoids the single point of failure of full custody while still allowing the provider to assist with recovery, for instance by re-issuing the patient's fragment after a verified identity check if her device is lost. For a health-data system intended to operate at the scale of India's population, and given the DPDP Act's own recognition, in its provisions on children's data and on persons with disabilities, that not every data principal can be assumed to exercise digital rights unaided, some variant of custodial or semi-custodial architecture is not a design failure but a practical necessity. The same point is reinforced by the right to nominate under Section 14 of the Act, which allows a data principal to nominate another individual to exercise her rights in the event of her death or incapacity, and which presupposes that, in a foreseeable class of cases, someone other than the patient will hold the means of exercising those rights.<sup>4</sup> The legal question this paper addresses is therefore not a marginal edge case but the structurally dominant scenario that any serious health-blockchain proposal in India will have to confront.

---

## VII. CONSENT, WITHDRAWAL, AND THE CRYPTOGRAPHIC REALITY OF REVOCATION

Having established how custody works technically, it is necessary to trace precisely what happens, at the level of the ledger, when a patient exercises her statutory right to withdraw consent, because the legal characterisation of the custodian's role depends on this mechanical detail rather than on loose analogy. On a blockchain, nothing already written to a confirmed block can be altered or deleted; this is the immutability property that gives the ledger its evidentiary value. Consent and its withdrawal are therefore not implemented by deleting a prior record but by appending a new transaction that supersedes it. A consent grant might take the form of a signed transaction creating a token or state entry that a given health information user is authorised to access a given category of the patient's records for a defined period and purpose. Withdrawal is implemented by a second signed transaction, referencing the first, that marks the authorisation as revoked. Any system checking access rights before serving a record must read the current state, which reflects the most recent valid transaction, rather than the original grant.

The decisive point is that both the original grant and the subsequent withdrawal require a valid cryptographic signature, and only the holder of the corresponding private key can produce one. If the patient does not hold that key, she cannot herself execute a withdrawal transaction on the ledger. She can only instruct whoever does hold the key to execute it on her behalf. This is not a peripheral technical detail; it is the precise point at which the patient's

---

<sup>4</sup>Digital Personal Data Protection Act 2023, s 14; Digital Personal Data Protection Rules 2025, G.S.R. 846(E) (13 November 2025), r 14(4).

statutory right of withdrawal under Section 6(4),<sup>5</sup> which entitles her to withdraw consent with ease comparable to that with which she gave it, is technically mediated through the custodian's willingness and capacity to act on her instruction. Where the custodian delays, refuses, or is simply unavailable, whether through insolvency, technical failure, or a dispute about the scope of the original instruction, the patient's statutory right is not merely inconvenienced but rendered practically inoperative, because there is no alternative technical route to executing the revocation herself.

A further complication arises from the mempool, the pool of signed but not yet confirmed transactions that every node in a network hold pending inclusion in the next block. Even once the custodian signs a withdrawal transaction on the patient's instruction, that transaction does not take effect the instant it is signed; it must propagate across the network and be included in a confirmed block, a process that on a permissioned health-data consortium chain using a Byzantine-fault-tolerant consensus mechanism will typically take seconds, but on a congested public chain could take substantially longer and is not fully within the custodian's control. Revocation is therefore not an instantaneous act but a process with a latency window during which a technically superseded, but not yet finally confirmed, authorisation could in principle still be read as valid by a system that has not yet synchronised to the latest block. Any custodian offering health-data consent services would need to build monitoring and confirmation-tracking into its operational obligations, and this operational burden is itself a further indicator, developed in Section X below, that the custodian is not a passive conduit but an active participant exercising judgment over how the patient's rights are given effect.

## VIII. THE ARCHITECTURE OF CONSENT UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 positions consent as the principal, though not the only, lawful basis for the processing of personal data, and Section 6 sets out in detail what counts as valid consent. Consent must be free, specific, informed, unconditional, and unambiguous, and must be indicated through clear affirmative action; any part of a consent that constitutes an infringement of the Act, the Rules made under it, or any other law in force is invalid to the extent of that infringement.<sup>6</sup> Section 6 further requires that any request for consent be presented in clear and plain language, with the data principal given the option to access it in English or in any language listed in the Eighth Schedule to the Constitution, and with contact details provided for a Data Protection Officer or other authorised person who can respond to the exercise of her rights. Critically for present purposes, the same section entitles the data principal to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which she gave it, and requires the Data Fiduciary, once consent is withdrawn, to cease processing, and to cause its Data Processors to cease processing, within a reasonable time unless processing without consent is required or authorised by law.<sup>7</sup>

The Act also creates, within Section 6 itself, a specific statutory intermediary through whom these rights may be exercised, the Consent Manager. A data principal may give, manage, review, or withdraw her consent to a Data Fiduciary through a Consent Manager, who is required to be accountable to the data principal and to act on her behalf, subject to obligations to be prescribed, and who, from the commencement of Section 6(9) and Rule 4, must be registered with the Data Protection Board under conditions set out in the Digital Personal Data Protection Rules, 2025.<sup>8</sup> This is a striking and, for the purposes of this paper, load-bearing feature of the statute, Parliament has already contemplated, and built a registered, regulated category for, an intermediary who exercises the data principal's consent rights on her behalf rather than the data principal exercising them directly. The statutory language describing the Consent Manager's role, that it must act on the data principal's behalf and be accountable to her, is agency language in substance if not in explicit statutory form (although, as Section XI shows, the First Schedule to the Rules then adds an express fiduciary duty), and it provides the closest existing analogue in Indian data protection law to the custodial wallet provider under examination here.

The Act's definitional architecture is equally important. Section 2(i) defines a Data Fiduciary as any person who, alone or in conjunction with other persons, determines the purpose and means of processing of personal data.<sup>9</sup> Section 2(k) defines a Data Processor as a person who processes personal data on behalf of a Data Fiduciary.<sup>10</sup> Processing itself, under Section 2(x), is defined broadly to include collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment, combination, indexing, sharing, disclosure, dissemination, and destruction of personal data, among other operations.<sup>11</sup> Taken together, these definitions establish a two-tier structure, an entity that merely carries out processing operations at another's direction is a processor, bound by contract to that other party's instructions and outside the primary compliance obligations of Chapter II, while an entity that

<sup>5</sup>Digital Personal Data Protection Act 2023, s 6(4).

<sup>6</sup>Digital Personal Data Protection Act 2023, s 6(1) (conditions of valid consent), s 6(2) (partial invalidity) and s 6(3) (clear and plain language, access in Eighth Schedule languages, and contact details).

<sup>7</sup>ibid ss 6(4) and 6(6).

<sup>8</sup>ibid ss 2(g) and 6(7)-(9); Digital Personal Data Protection Rules 2025, G.S.R. 846(E) (13 November 2025), r 4.

<sup>9</sup>Digital Personal Data Protection Act 2023, s 2(i).

<sup>10</sup>ibid s 2(k).

<sup>11</sup>ibid s 2(x); on the definition of 'personal data', see s 2(t).

determines why and how processing occurs, whether alone or jointly with others, is a fiduciary, bearing the full weight of notice, consent-validity, security-safeguard, and grievance-redress obligations under the Act. The remainder of this paper is, in substance, an exercise in locating the custodial key-holder within this two-tier structure, or in demonstrating that the structure as currently drafted does not cleanly accommodate it.

### *Commencement and Temporal Scope*

The analysis in this paper is prospective, because the Act and the Rules commence in phases. The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025. Under Rule 1, Rules 1, 2 and 17 to 21 took effect on publication, Rule 4 comes into force one year after publication, and Rules 3, 5 to 16, 22 and 23 come into force eighteen months after publication.<sup>12</sup> The commencement notification for the Act follows the same pattern. Section 2 and the provisions establishing the Data Protection Board took effect on 13 November 2025; Section 6(9) of the Act, which requires every Consent Manager to be registered with the Board, and the Board's corresponding power under Section 27(1)(d) follow after one year; and the remaining provisions, including Sections 3 to 5, Section 6(1) to (8) and (10), Sections 7 to 17 and the penalty provisions, follow after eighteen months.<sup>13</sup> Counting from the Gazette publication date of 13 November 2025, Consent Manager registration under Rule 4 therefore begins on 13 November 2026, and the principal processing, rights, and penalty provisions, together with the Rules that give them operational content, begin on 13 May 2027. Until then no Consent Manager can be registered under Rule 4, and the duties of a Data Fiduciary discussed in this paper, including the full suite of Chapter II obligations that the central argument attaches to a custodian, are duties that will attach from 13 May 2027 and not obligations that presently bind custodians. The Data Protection Board is established under Section 18 of the Act with effect from 13 November 2025, but published commentary through the third quarter of 2026 indicates that its Chairperson and Members had yet to be appointed, and this paper accordingly treats the Board's registration and guidance functions as prospective.

## **IX. LOCATING THE AGENT, CUSTODIAL WALLET PROVIDERS AND THE LAW OF AGENCY**

Before reaching the specifically statutory question of fiduciary status under the DPDP Act, it is worth pausing on the antecedent, general private-law question of what kind of legal relationship arises between a patient and a custodial key-holder, because that relationship shapes the duties the custodian owes even independent of data protection legislation. The Indian Contract Act, 1872 defines an agent, under Section 182, as a person employed to do any act for another, or to represent another in dealings with third persons, and the person for whom such act is done is the principal.<sup>14</sup> Section 186 recognises that the authority of an agent may be express or may be implied from the circumstances of the case.<sup>15</sup> Sections 211 to 213 impose on the agent a duty to conduct the business of the agency according to the principal's directions, and to act with the skill and care that is reasonably expected, failing which the agent must compensate the principal for resulting loss, and to render proper accounts to the principal on demand.<sup>16</sup>

A custodial wallet provider that holds a patient's private key and signs transactions in response to instructions communicated through an application, a call-centre channel, or an agent-assisted enrolment process fits this description closely. The provider does an act, namely signing and broadcasting a transaction, for the patient, and does so in order to represent her interests in a dealing with a third party, namely the hospital or health information user whose access is being granted or revoked. The authority may be express, as where the patient taps a button in an application to grant access to a named clinic, or implied, as where a standing instruction to grant emergency responders access during a medical crisis is executed automatically according to pre-set rules the patient earlier approved. On ordinary principles, the provider owes the patient the duties of skill and fidelity that Sections 211 to 213 impose on any agent, quite apart from anything the DPDP Act separately requires.

It is worth distinguishing this characterisation from two others that might superficially seem apt. The first is bailment, one might think of the custodian as merely storing an object, the private key, on the patient's behalf, in the way a locker service stores a physical item without exercising any judgment about its use. This characterisation captures the storage function but misses the far more consequential fact that the custodian does not merely hold the key inertly; it actively uses the key, at the patient's instruction, to alter the state of a public or consortium ledger with legal and clinical consequences. A bailee who used the bailed property to transact on the bailor's behalf, rather than simply safekeeping it, would in Indian law typically be treated as having stepped into an agency relationship for the purposes of that use, which is precisely the situation of a signing custodian. The second candidate characterisation is trusteeship, under which the custodian would hold the key as trust property for the patient's benefit, subject to the fiduciary standards

<sup>12</sup>Digital Personal Data Protection Rules 2025, G.S.R. 846(E) (13 November 2025), r 1(2)-(4).

<sup>13</sup>Ministry of Electronics and Information Technology, notification of 13 November 2025 appointing the dates on which the provisions of the Digital Personal Data Protection Act 2023 come into force (G.S.R. 843(E)).

<sup>14</sup>Indian Contract Act 1872, s 182.

<sup>15</sup>ibid s 186.

<sup>16</sup>ibid ss 211-213.

of the Indian Trusts Act, 1882.<sup>17</sup> This framing is attractive because it, too, imports fiduciary-style duties, but it fits less well, for two reasons. The first and stronger reason is structural. A trust is, under the Indian Trusts Act, 1882, an obligation annexed to the ownership of property, and the beneficiary's beneficial interest is her right against the trustee as owner of the trust property; a trust of movable property, moreover, is valid only if it is declared in the manner the Act requires or if ownership of the property is transferred to the trustee.<sup>18</sup> A custodian that holds a key for the patient normally owns neither the key nor the patient's health data, so there is no trust property of which it is the owner and no transfer of ownership to it. The second reason is functional, a trustee typically holds ownership of, and exercises independent discretion over, the trust property itself, whereas a well-designed custodial wallet is meant to exercise no discretion at all over the key's use beyond executing the patient's specific instructions. Agency, rather than bailment or trusteeship, is accordingly the better doctrinal fit for the paradigm case of an instruction-following custodian, though as the next section shows, the moment a custodian begins to exercise independent discretion over how processing occurs, the analysis shifts and a fiduciary characterisation, in both the trust-law and the DPDP Act sense, becomes appropriate.

## **X. DOES CUSTODIAL KEY-HOLDING TRIGGER DATA FIDUCIARY STATUS? TESTING THE WALLET PROVIDER AGAINST SECTION 2(I)**

The private-law finding that a custodial wallet provider is ordinarily an agent of the patient does not by itself answer the separate, statutory question of whether that provider is also a Data Fiduciary under the DPDP Act, because agency and fiduciary status under the Act are governed by different tests and can, in principle, diverge. The statutory test in Section 2(i) turns on whether the entity determines the purpose and means of processing, alone or in conjunction with others, not on whether it acts as someone's agent in the general law sense. It is entirely possible for an agent, in the contract-law sense, to be a mere processor under the Act, provided it exercises no independent discretion over why or how processing occurs and simply executes precise instructions.

The first step in applying the statutory test is to establish that what the custodian handles is personal data at all, since Section 2(i) only bites on the processing of personal data. The patient's private key is not, in itself, health information, but the key, the transaction metadata it generates, and the pattern of which addresses it signs transactions with are all data that relate to an identifiable patient, and under the Act's broad definition of personal data in Section 2(t), this metadata is capable of qualifying as personal data in its own right, independent of the clinical content that remains off-chain. A record showing that a particular patient's key signed an access grant to a particular oncology clinic at a particular time is itself a piece of sensitive information about that patient, even before the underlying medical file is examined, and its handling by the custodian is accordingly processing within the meaning of the Act.

The second and decisive step is to ask whether the custodian determines the purpose and means of that processing or merely executes the patient's own determinations. Where a custodian's function is limited strictly to receiving a specific, patient-originated instruction, such as grant access to Dr. Mehta for thirty days, translating it faithfully into a signed transaction, and broadcasting it, the custodian is not determining purpose or means in any meaningful sense; the patient has determined both, and the custodian is functioning as a processor under Section 2(k), analogous to a bank that executes a customer's payment instruction without independently deciding to whom or why the money is sent. On this narrow instruction-execution function alone, the case for fiduciary status is weak, and treating every custodial wallet provider as a full Data Fiduciary merely because it holds signing keys would over-extend the statute and discourage the development of the very custodial infrastructure that population-scale health-data access requires.

That conclusion leaves open an antecedent question that the statutory definition forces, for whom does the instruction-following custodian act as processor? Section 2(k) defines a Data Processor as a person who processes personal data on behalf of a Data Fiduciary, and the patient, as Data Principal, is not a Data Fiduciary. Three answers are possible. The first is that the custodian processes on behalf of the health information provider or network operator that determines why and how the patient's records are processed, so that it is a processor of that Fiduciary even though the instruction it executes originates with the patient. The second is that the custodian acts as the patient's agent in the general-law sense and falls outside the processor category altogether, so that its functions are not processing on behalf of a Data Fiduciary at all and are caught by the Act, if at all, only through the Section 2(i) test. The third is that the custodian is a fiduciary for the key-custody function itself, because the handling of the key and of the transaction metadata is a processing activity whose purpose and means the custodian, and neither the patient nor the health information provider, in practice determines. The choice has consequences under Section 8, which makes a Data Fiduciary responsible for complying with the Act in respect of processing undertaken on its behalf by a Data Processor irrespective of any agreement to the contrary, and which permits a Data Fiduciary to involve a Data Processor for activities related to offering goods or services to Data Principals only under a valid contract.<sup>19</sup> The first option places the custodian within a chain of contractual

<sup>17</sup>Indian Trusts Act 1882, s 3.

<sup>18</sup>Indian Trusts Act 1882, ss 3 and 5.

<sup>19</sup>Digital Personal Data Protection Act 2023, s 8(1)-(2).

responsibility that already exists in ABDM-style architectures; the second leaves a gap in the Act's coverage; and the third converts an instruction-following function into a fiduciary one. Section XIV tests the three-part framework against each option in turn.

But real custodial wallet providers rarely confine themselves to bare instruction execution, and it is here that the analysis must become functional rather than formal. A provider that sets a default retention period for key backups without patient-specific instruction, that establishes standing rules for emergency or default access in the absence of an explicit patient instruction, that bundles consent flows so that granting access to one class of provider automatically extends to another, or that analyses transaction-level metadata, for instance the frequency or pattern of access requests, for its own commercial purposes such as building risk profiles to sell to insurers or building engagement analytics to sell advertising, has moved decisively beyond execution into determination. In each of these examples the provider is deciding, on its own initiative and not at the patient's specific direction, why or how processing occurs, which is exactly the statutory formula in Section 2(i), and it does so in conjunction with the underlying health information provider or user, which is precisely the joint-determination scenario the phrase in conjunction with other persons was drafted to capture. On this functional test, such a provider is a Data Fiduciary with respect to those specific processing activities, and will be fully subject, once Chapter II commences, to the notice, consent-validity, purpose-limitation, and security-safeguard obligations of that Chapter, regardless of whether it also happens to be, at general law, the patient's agent for the narrower task of signing transactions.

The upshot is that mere possession of the signing key is not itself the trigger for fiduciary status; the exercise of unilateral discretion over the terms of processing is. This distinction matters practically because it allows regulators and courts to distinguish genuinely patient-controlled custodial infrastructure, which should be encouraged as a proportionate response to the digital-literacy and key-loss problems described in Section VI, from custodial infrastructure that uses the technical necessity of holding keys as a pretext for accumulating discretionary control over how a patient's most sensitive data moves through the health system.

---

## XI. THE CONSENT MANAGER ANALOGY AND ITS LIMITS

Section VIII noted that the DPDP Act already creates a registered, regulated category of intermediary, the Consent Manager, whose statutory description, acting on the data principal's behalf and remaining accountable to her, closely tracks the function performed by a custodial health-data wallet provider that executes consent grants and withdrawals on a patient's instruction. This convergence is not accidental, and it suggests a doctrinal move that this paper argues should be taken seriously, where a custodial wallet provider's discretionary functions, identified under the test in Section X, substantially replicate the statutory role of giving, managing, reviewing, or withdrawing consent on the data principal's behalf, that provider is, in substance, performing the function the Act assigns to a Consent Manager, and should be required to register and operate under the conditions the Digital Personal Data Protection Rules, 2025 impose on Consent Managers under Rule 4,<sup>20</sup> rather than being permitted to perform an equivalent function under a different technical label and thereby escape the interoperability, transparency, and Board-oversight conditions that registration entails.

The risk this analogy is meant to guard against is a straightforward form of regulatory arbitrage, an entity that would plainly be a Consent Manager if it presented itself as a consent-management dashboard could, by re-describing its identical function as a cryptocurrency-style wallet holding keys rather than a consent record holding permissions, present a colourable argument that it falls outside the Consent Manager framework entirely while performing exactly the function that framework was built to regulate. Indian administrative and tax law has long applied a substance-over-form approach to arrangements that use formal labels to escape a regulatory category their underlying function plainly satisfies, and there is no principled reason data protection regulation should be more indulgent of label-driven arbitrage than other regulatory fields are.

The analogy nonetheless has real limits that a careful doctrinal account must acknowledge rather than paper over. The Consent Manager framework, as presently structured under the Rules, was drafted with a relatively conventional consent-dashboard model in mind, one in which the Consent Manager aggregates and displays consent status across multiple data fiduciaries without itself holding any cryptographic instrument that is the sole technical means of exercising the underlying right. A custodial wallet provider's function is broader than this in one respect, because it does not merely record or display the patient's consent decisions but is the exclusive technical mechanism through which those decisions take cryptographic effect; and it may be narrower in another respect, because a wallet provider serving a single blockchain-based health network may not offer the cross-fiduciary interoperability that the Consent Manager Rules appear to contemplate as a defining feature. There is accordingly a genuine gap between the existing regulatory category and the technical reality of key custody that this paper can identify but cannot itself close; that closure properly belongs to the Data Protection Board, through guidance or subordinate rulemaking that addresses key-custody-based consent execution as either a variant of the existing Consent Manager category or as a distinct, appropriately regulated category of its own.

---

<sup>20</sup>Digital Personal Data Protection Rules 2025, G.S.R. 846(E) (13 November 2025), r 4 (n 8).

The limits become sharper once the First Schedule to the Rules is read against the analogy. Section 2(g) of the Act defines a Consent Manager as a person registered with the Board who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw her consent through an accessible, transparent, and interoperable platform, and Section 6(9) makes registration a condition of being one.<sup>21</sup> Part A of the First Schedule conditions registration on, among other things, incorporation as a company in India, sufficient technical, operational, and financial capacity, a net worth of not less than two crore rupees, independent certification that the applicant's interoperable platform is consistent with the data protection standards and assurance framework published by the Board, and charter provisions that secure the conflict-of-interest obligations in Part B. Part B then imposes continuing obligations, three of which bear directly on the analogy, the Consent Manager must ensure that the manner of making available or sharing personal data is such that its contents are not readable by it; it must not sub-contract or assign the performance of any of its obligations under the Act and the Rules; and it must act in a fiduciary capacity in relation to the Data Principal.<sup>22</sup>

Each of those three conditions is difficult for a key-holding custodian to satisfy in the form in which this paper describes it. The non-readability condition is directed at the personal data being shared, and a custodian that signs consent transactions need not read the clinical content, which remains off-chain; but a custodian necessarily processes the consent metadata it signs, and a full-custody model, under which the custodian generates and stores the key on its own infrastructure, places in its hands the means to decrypt any content that is encrypted to the corresponding public key. Whether such a custodian can meet the condition therefore depends on architecture, and in particular on whether the key is used only to sign and never to decrypt, a design question that threshold or multi-party computation schemes can address in part. The bar on sub-contracting sits uneasily with custodians that rely on cloud infrastructure or hardware security module vendors to generate, store, and use keys, because those vendors perform part of the custodian's function in a practical sense; whether the bar reaches the procurement of infrastructure, as distinct from the assignment of the Consent Manager's regulatory obligations, is a question the Rules do not answer. And the express fiduciary duty changes the characterisation offered in Section VIII, the Rules do not merely describe the Consent Manager as an agent accountable to the Data Principal, they require it to act in a fiduciary capacity in relation to her, which is a stronger and different standard from the duties of skill and fidelity that Sections 211 to 213 of the Indian Contract Act impose on an agent. A custodian that is brought within the Consent Manager category by the registration-convergence rule therefore does not remain a mere agent for that function; it takes on a fiduciary duty of the express kind, whatever its classification under the general law.

Finally, because Section 2(g) defines a Consent Manager as a person registered with the Board, a custodian does not become a Consent Manager by performing the function; it becomes one only by registering. Convergence by substance alone therefore cannot carry the argument unaided. It needs the support of the Board, through guidance within its powers, and of the Central Government, through its rule-making power under Section 40 of the Act, to say either that custodians whose discretionary functions replicate the Consent Manager role must register, or that they fall into a distinct category with conditions adapted to key custody. Until then, the registration-convergence rule is best understood as a claim about how the Board and the Ministry should treat custodians whose functions overlap with the statutory role.

---

## **XII. COMPARATIVE REFLECTIONS, THE GDPR CONTROLLER-PROCESSOR LINE AND CUSTODIAL CRYPTO-ASSET REGULATION**

The structural problem addressed in this paper is not unique to India, and a brief comparative detour clarifies what is genuinely novel about the blockchain-custody scenario and what is simply a familiar problem in new clothing. The European Union's General Data Protection Regulation draws a distinction, in Articles 4(7) and 4(8),<sup>23</sup> between a controller, who determines the purposes and means of processing, and a processor, who processes data on the controller's behalf, a distinction that maps closely onto the DPDP Act's fiduciary-processor split and was, as a matter of legislative history, one of its acknowledged influences. European data protection authorities, including the French Commission Nationale de l'Informatique et des Libertés, have already grappled with attributing controller status across the distributed participants of a blockchain network. The CNIL's 2018 analysis treats a participant who has the right to write to the chain, and who decides to send data for validation, as capable of being a controller, because such a participant defines the purposes and means of the processing; it treats miners that merely validate transactions as not determining those purposes and means, and so as not controllers, although in some cases they may be processors acting on the participants' instructions; and it treats a smart contract developer who intervenes in the processing on a participant's behalf as potentially a processor.<sup>24</sup> The European Data Protection Board's final Guidelines 02/2025, adopted on 7 July 2026 after public consultation, take a similarly functional approach. They require a factual assessment of roles for each processing activity; accept that

---

<sup>21</sup>Digital Personal Data Protection Act 2023, ss 2(g) and 6(9).

<sup>22</sup>Digital Personal Data Protection Rules 2025, G.S.R. 846(E) (13 November 2025), First Schedule, pt A (items 1, 2, 4, 7 and 9) and pt B (items 2, 6 and 8).

<sup>23</sup>Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 4(7)-(8).

<sup>24</sup>Commission Nationale de l'Informatique et des Libertés, 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data' (CNIL, September 2018).

nodes performing only technical validation, without deciding purposes and essential means, might not be controllers; accept that nodes exercising a decisive influence over purposes and essential means may be controllers or joint controllers; and, for public permissionless networks in which nodes exercise that influence, strongly encourage the establishment of a consortium or other legal entity that would act as controller.<sup>25</sup> The two positions differ in one respect that matters here, the CNIL treats validating miners as outside controllership, whereas the EDPB accepts that in some networks validating nodes may be controllers or joint controllers. They converge on the value of an identifiable, accountable legal entity as controller where several participants act together. This confirms, from a different regulatory tradition, the functional rather than purely formal approach this paper has argued for under Section 2(i), decentralisation of infrastructure does not by itself decentralise legal responsibility, and whoever exercises real discretion over how the system operates remains identifiable and accountable. The comparison also assists the argument made here. A custodian that is a legal person and writes consent transactions to a chain occupies the 'participant' position, and on the CNIL's approach a participant of that kind is a candidate controller; the functional test proposed in this paper refines that presumption by asking whether, in executing a given transaction, the custodian decides purposes and means or merely carries out the patient's determination, which is the question that the instruction-fidelity and discretion-locus tests in Section XIV ask. The EDPB's encouragement of an accountable legal entity also parallels this paper's call, in Section XV, for an identifiable and accountable custodial entity.

A second, and in some ways more directly relevant, comparative reference point comes not from data protection law at all but from financial regulation of custodial crypto-asset service providers. Global standard-setters including the Financial Action Task Force,<sup>26</sup> and regional frameworks such as the European Union's Markets in Crypto-Assets Regulation,<sup>27</sup> already impose on custodians of crypto-asset private keys a distinct set of duties independent of any data protection analysis, obligations to segregate customer assets from the custodian's own holdings, to maintain verifiable records of whose keys are held and on what instructions they were used, and to bear a heightened standard of care commensurate with the fact that the custodian's possession of the key gives it practical, if not beneficial, control over the customer's asset. These obligations arise not because the custodian is deemed to own the asset, but because the custodian's technical control creates exactly the kind of asymmetric power over another person's property that fiduciary-style duties have always existed to discipline. The parallel to health-data key custody is close, a custodian holding a patient's signing key has practical, though not beneficial, control over the patient's exercise of a fundamental data-protection right, and the same underlying rationale, that technical control over an access-credential to a valuable or sensitive asset warrants enhanced legal duty regardless of the label the custodian gives itself, transfers cleanly from the financial-custody context to the health-data context even in the absence of dedicated crypto-custody legislation in India specifically directed at this scenario.

### **XIII. APPLICATION, HEALTH-DATA WALLETS IN THE AYUSHMAN BHARAT DIGITAL MISSION CONTEXT**

It should be stated plainly that the Ayushman Bharat Digital Mission, as presently implemented, does not run its Health Information Exchange and Consent Manager architecture on a blockchain; its consent-management layer is centrally orchestrated, built around the Ayushman Bharat Health Account identifier and a set of Consent Managers operating under the Mission's own framework rather than on a distributed ledger.<sup>28</sup> Those Consent Managers are distinct from the Consent Managers that Section 6(9) of the Act and Rule 4 will require to be registered with the Board, and no Consent Manager can be registered under Rule 4 until it commences.<sup>29</sup> The Mission is nonetheless the natural setting in which the argument developed here will eventually be tested, both because any private-sector entity that layers a blockchain-based audit trail or consent-execution mechanism on top of the Mission's existing rails, for the tamper-evidence and interoperability reasons discussed in earlier work on this subject, will have to interoperate with the Mission's Health Information Provider and Health Information User architecture, and because the Mission's own design already accepts the premise, central to this paper, that most patients will exercise their consent rights through an intermediary application rather than through direct, unmediated technical control.

Consider, as an illustration, a hypothetical wallet application, deployed in partnership with a state health mission to serve elderly and low-literacy patients in a rural district, that custodies each patient's signing key on encrypted infrastructure and executes consent grants and withdrawals on the patient's

<sup>25</sup>European Data Protection Board, 'Guidelines 02/2025 on processing of personal data through blockchain technologies' (Version 2.0, adopted 7 July 2026) paras 36-44. See also European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (Version 2.1, adopted 7 July 2021).

<sup>26</sup>Financial Action Task Force, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (FATF, October 2021).

<sup>27</sup>Regulation (EU) 2023/1114 on Markets in Crypto-Assets [2023] OJ L150/40.

<sup>28</sup>National Health Authority, 'Health Data Management Policy' (Version 1.0, December 2020); National Health Authority, 'Draft Health Data Management Policy' (Version 02, consultation draft, 23 April 2022); National Health Authority, 'National Digital Health Mission: Strategy Overview' (2020).

<sup>29</sup>Digital Personal Data Protection Act 2023, s 6(9); Digital Personal Data Protection Rules 2025, G.S.R. 846(E) (13 November 2025), rr 1(3) and 4.

spoken instruction, communicated through a village-level health worker or a call-centre channel, rather than through direct interaction with a smartphone interface. Applying the framework built across Sections IX and X, the application is, at general law, the patient's agent for the specific function of signing instructed transactions, and its personnel owe the ordinary duties of skill and fidelity that agency entails. Whether it is also a Data Fiduciary under the DPDP Act turns on whether its functions remain confined to faithful instruction-execution or extend into autonomous determination. If the application, for operational necessity, establishes a default rule that emergency responders may access a minimal data set without a fresh instruction in every case, or if it retains transaction logs for a period it sets unilaterally rather than one specified by the patient or required by law, it may, with respect to those specific functions, cross into fiduciary territory, while remaining a mere processor with respect to the narrower function of executing an explicit, patient-specific access grant. Whether it does so depends, for each function, on how far the Act and the Rules already fix the answer, and two provisions matter in particular.

The first is Section 7(f) of the Act, which permits a Data Fiduciary to process personal data without consent for the purpose of responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual.<sup>30</sup> The ground is available to a Data Fiduciary, and it therefore matters who invokes it and who decides that an emergency exists. Where the health information provider or user determines that an emergency exists and requests access, a custodian that releases the minimal data set on that request is carrying out the Fiduciary's determination, and for that function it remains within the processor category. Where, by contrast, the custodian's own standing rule decides in advance that a class of circumstances amounts to an emergency, and releases data on that basis without a Fiduciary's request or the patient's instruction, the custodian is itself deciding when the Section 7(f) ground is engaged. That decision is an exercise of discretion over the terms of processing of the kind the discretion-locus test targets, and a blanket default rule that cannot be tied to a genuine threat to life or immediate threat to health sits uneasily with a ground that is confined to those circumstances.

The second is the retention regime in the Rules. Rule 8(3) requires a Data Fiduciary to retain personal data, associated traffic data, and other logs of processing, whether undertaken by it or on its behalf by a Data Processor, for a minimum of one year from the date of processing, for the purposes specified in the Seventh Schedule, and Rule 6(1)(e) separately requires, as part of the minimum security safeguards, the retention of logs and personal data for one year to enable the detection and investigation of unauthorised access, unless other law requires otherwise.<sup>31</sup> Both rules commence on 13 May 2027. The retention example therefore has to be divided. A period that reflects these statutory minimums is set by law and not by the custodian, and it does not make the custodian a fiduciary; a custodian that retains transaction logs or key-backup material beyond those minimums, for a period of its own choosing and for purposes the patient did not specify, exercises discretion over the terms of processing for that further period.

Re-running the discretion-locus test on these facts produces a narrower and more precise result than a bare reference to default access and retention would suggest. The execution of an explicit, patient-specific grant remains an instruction-fidelity function, and the custodian is a processor for it. Its release of data on a Fiduciary's Section 7(f) request remains within the Fiduciary's determination. Its own standing rule on when an emergency exists, and its choice of a retention period beyond the statutory minimum, remain functions in which the custodian determines purpose or means, and for those functions only it satisfies Section 2(i) of the Act.

This dual characterisation, processor for some functions and fiduciary for others within the same entity, is not a doctrinal awkwardness to be resolved in favour of one label or the other; it is, this paper argues, the doctrinally correct description of how most real custodial health-data wallets will actually operate, and Indian and comparative law already permit exactly this kind of function-specific characterisation, since both the DPDP Act and the GDPR contemplate a single entity holding processor status for some processing activities and controller or fiduciary status for others, provided the two roles are kept analytically and, ideally, operationally distinct. A rural health-wallet operator built along these lines would need to conduct its own internal mapping of which functions are pure execution and which involve autonomous decision-making, apply the full weight of Chapter II obligations, including valid notice, security safeguards, and grievance redress, only to the latter, and, per the argument in Section XI, assess whether its discretionary functions are substantial enough to require Consent Manager registration under Rule 4 of the 2025 Rules.

---

#### XIV. DOCTRINAL SYNTHESIS, A PROPOSED LIABILITY FRAMEWORK

Drawing the preceding analysis together, this paper proposes a three-part framework for locating the legal status of a custodial key-holder in a blockchain-based health-data system, intended to be applicable both to disputes that reach the Data Protection Board and to the design choices of entities building such systems in the first place. The first element is an instruction-fidelity test, for each discrete function the custodian performs, from key generation

---

<sup>30</sup>Digital Personal Data Protection Act 2023, s 7(f).

<sup>31</sup>Digital Personal Data Protection Rules 2025, G.S.R. 846(E) (13 November 2025), rr 6(1)(e) and 8(3) and Seventh Schedule.

through transaction signing to backup and recovery, one asks whether the custodian acts strictly according to a specific, patient-originated instruction, exercising no independent judgment about whether, when, or on what terms the instructed act should occur. Functions that pass this test are processing carried out on the data principal's, or more precisely on the underlying health information provider's, behalf, and the custodian's role with respect to them is that of a Data Processor under Section 2(k), coupled with the general-law duties of an agent under Sections 182 and 211 to 213 of the Indian Contract Act.

The second element is a discretion-locus test, applied to any function that fails the first test. Here one identifies precisely where and how the custodian exercises autonomous judgment, whether in setting default access rules, determining retention periods for key material or transaction logs, bundling or pre-configuring consent scopes, or deriving and using transaction-level metadata for purposes the patient did not specifically authorise. With respect to each such function, and only that function, the custodian satisfies the purpose-and-means test in Section 2(i) and becomes a Data Fiduciary, bearing, from the commencement of Chapter II, the corresponding notice, consent-validity, and safeguard obligations. This function-specific attribution avoids the two failure modes that a cruder, all-or-nothing approach would produce, treating every custodian as a full fiduciary would discourage the development of custodial infrastructure that vulnerable patients structurally need, given the key-loss problem described in Section VI, while treating every custodian as a mere processor would allow entities to accumulate substantial discretionary control over the exercise of a constitutional and statutory right while disclaiming all fiduciary accountability for it.

The third element is a registration-convergence rule, addressed to the specific overlap identified in Section XI. Where an entity's discretionary functions, assessed under the second element, substantially replicate the statutory role of giving, managing, reviewing, or withdrawing consent on a data principal's behalf, whether it labels itself a wallet, a custodian, or anything else, it should be treated as performing the function the Act assigns to a registered Consent Manager and should accordingly be required to satisfy the registration and operational conditions the Digital Personal Data Protection Rules, 2025 impose under Rule 4 and the First Schedule, subject to whatever technical adaptation of those conditions the Data Protection Board considers appropriate for a key-custody-based, rather than a dashboard-based, consent-execution model. Until the Board or the Ministry of Electronics and Information Technology issues specific guidance addressing this convergence, this paper submits that the substance-over-form principle already implicit in the Act's purposive definitions provides a doctrinal basis for applying Consent Manager-equivalent scrutiny to any custodial key-holder whose discretionary functions meet this threshold, as a matter of how the Board should exercise its supervisory functions and how the Ministry should frame its guidance, rather than waiting for a gap in subordinate legislation to be closed before the underlying accountability question is addressed. Registration itself is a legal status that can follow only from the Act and the Rules, because Section 2(g) defines a Consent Manager as a person registered with the Board, and any technical adaptation of the Part B conditions would have to address the non-readability condition, the bar on sub-contracting, and the express fiduciary duty discussed in Section XI.

The framework does not depend on resolving the question, identified in Section X, of the party on whose behalf an instruction-following custodian acts as processor. If the custodian is a processor of the health information provider or network operator, the first element identifies the functions that sit within that relationship, the Fiduciary remains responsible for them under Section 8(1), and the second element identifies the functions, outside any instruction, for which the custodian is a Data Fiduciary in its own right. If the custodian is instead the patient's agent and outside the processor category, the first element still sorts functions by instruction-fidelity, but the regulation of the functions that pass it rests on agency doctrine and on the duties imposed by Sections 211 to 213 of the Indian Contract Act, which is the principal reason the second and third elements matter, they ensure that the functions that fail the test are not left unregulated by reason of that classification. If the custodian is a fiduciary for the key-custody function as a whole, the framework yields a more demanding result than the one defended here, because the whole function, including faithful instruction-execution, would be treated as one in which the custodian determines purpose and means, and the reasons given above for rejecting an all-or-nothing approach apply to that result.

---

## XV. SUGGESTIONS AND RECOMMENDATIONS

The analysis above identifies a regulatory gap and offers an analytical framework, but the framework does not by itself tell the authorities or system designers what to do. This Part therefore makes four sets of proposals.

First, the Data Protection Board, once constituted, and the Ministry of Electronics and Information Technology, in the exercise of its rule-making and guidance functions, should issue guidance on key-custody-based consent execution. The guidance should state that possession of a signing key is not by itself determinative of fiduciary status; should adopt the function-by-function approach of the instruction-fidelity and discretion-locus tests; and should identify examples of discretionary functions, such as default access rules, custodian-set retention periods, bundled consent scopes, and secondary use of transaction metadata, that make a custodian a Data Fiduciary for those functions.

Second, the Ministry, with the Board, should decide whether custodians whose discretionary functions replicate the statutory Consent Manager role must

register as Consent Managers, or whether they form a separate category of regulated key-custody consent executors with adapted conditions. The decision should confront the First Schedule conditions identified in Section XI, namely non-readability, the bar on sub-contracting, and the express fiduciary duty, and should state how they apply to custodians that rely on cloud or hardware security module vendors. Because Rule 4 commences on 13 November 2026, ahead of the main obligations, the decision should be made before registrations are processed, so that applicants know whether key custody falls inside or outside the category.

Third, designers and operators of custodial wallets should build the functional separation on which the framework depends. They should map each function, from key generation through signing, backup, recovery, and retention, as either instruction-execution or discretionary; log, for each execution function, the patient-originated instruction to which the signed transaction corresponds, so that instruction-fidelity can be demonstrated and the same record made available to the patient; adopt threshold or multi-party signing where feasible, so that the custodian cannot sign without the patient's key fragment; avoid using signing keys to decrypt clinical content; fix retention periods by reference to the statutory minimums and disclose any longer period and its purpose; and record, for any access granted on the ground of medical emergency, which Fiduciary determined that an emergency existed and on what basis.

Fourth, the National Health Authority should align its Ayushman Bharat Digital Mission documents with the Act and the Rules. The documents on which the Mission's consent architecture presently rests pre-date the commencement of the Act, the Health Data Management Policy was published in December 2020, and the revised version circulated in April 2022 was a consultation draft. The Authority should state, at a minimum, how the Mission's own Consent Manager arrangements relate to Consent Managers registered with the Board under Rule 4, how emergency access under the Mission's rules relates to Section 7(f) of the Act, and how log retention under those rules relates to Rules 6 and 8.

---

## XVI. CONCLUSION

The deeper argument advanced in this paper is that the self-sovereignty promise at the heart of blockchain-based health-data design, however genuine its underlying commitment to patient autonomy, does not survive first contact with the realistic requirement of population-scale deployment intact. Key loss is not a marginal risk to be mitigated at the edges of an otherwise self-sovereign system; it is a structural certainty for a meaningful proportion of any large and digitally heterogeneous patient population, and the only serious engineering response to that certainty is some form of custodial or semi-custodial key management. What this means, in doctrinal terms, is that blockchain architecture does not eliminate intermediaries from health-data governance; it relocates them, from the data controllers and processors that conventional data protection law was built to regulate, to key custodians whose formal function, safekeeping and using a cryptographic credential, sits awkwardly astride the existing categories of agent, processor, and fiduciary.

Indian data protection law, and specifically the Digital Personal Data Protection Act, 2023, was drafted against the backdrop of a pre-blockchain data architecture in which the entity determining why and how personal data is processed is usually easy to identify by looking at who runs the database. That assumption does not fail in a blockchain-based system so much as it requires a more granular application, the relevant question is no longer simply which entity runs the system, but which entity, among potentially many technical participants, exercises genuine discretion over the terms on which a patient's statutory rights are given cryptographic effect. This paper has argued that mere possession of a signing key does not answer that question; the exercise of autonomous discretion over retention, default access, bundling, or data-derived analytics does, and that a function-specific rather than an entity-wide approach to fiduciary characterisation, combined with a substance-over-form extension of the existing Consent Manager framework, offers a workable path for the Data Protection Board and for system designers alike. The recommendations in Section XV identify the guidance, decisions, and design practices through which that path could be made operational. Until such guidance is formalised, entities building custodial health-data wallets in India would be well advised to conduct exactly the functional self-audit proposed in Section XIV before assuming that the technical label of a wallet, rather than a consent manager, is sufficient to place them outside the reach of Chapter II of the Act.