Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The Consent Manager as Authority Graph: Capturing Consent under DPDPA 2023

Manika Sharma
National Law University Jodhpur

Abstract **- The Digital Personal Data Protection Act 2023 and the Digital Personal Data Protection Rules 2025 oblige every Data Fiduciary to capture verifiable consent from the Data Principal, and where the Principal is a child or a person with disability, from an authority the statute recognises as lawful. Rule 11 of the DPDP Rules names three such authorities, namely a court of law, a designated authority under section 15 of the Rights of Persons with Disabilities Act 2016 (RPwD), and a local level committee constituted under the National Trust for Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (National Trust Act). Schedule IV adds five scope restricted Data Fiduciary classes and five exempt purposes, each riding on its own source of authority. This article argues that the workable Consent Manager under the DPDPA is not a repository of consent receipts but a typed authority graph whose edges are bounded in time. Put simply, a consent manager is more than static space for consent collection, instead it is a dynamic network map of permissions. Where node/dots is a representation of entities such as data principal, natural persons acting on behalf of the data principal, data fiduciary, data processor, authorities like DigiLocker, Court, local committee, etc. And, edge is a representation of the signed permissions that connect one node/dot to another. These arrows are labelled with purpose and time-bounded. Lastly, a token is a small piece of signed data issues by an authority that certifies the existence of an edge-relations, thus forming the issuance layer. The graph portrays the consent map through which the consent manager can walk through. The graph is also what makes the revocation cascade possible. When an edge dies, the graph can traverse outward along the processes-for and derived-from edges and tell every downstream node to stop. That traversal is only possible because all the nodes and edges live inside one connected structure.**

Keywords—Digital Personal Data Protection Act, Consent Manager, Authority Graph, Verifiable Consent, DPDP Rules 2025.

I. INTRODUCTION

Who counts as a Data Principal whose consent a Data Fiduciary must capture? Who counts as the person whose signature binds that Principal when she is a child, or a person with disability whose guardian the law recognises? Who counts as the authority that speaks for her when the statute offers not one route but several, a civil court, a designated authority under section 15 of the Rights of Persons with Disabilities Act 2016 (RPwD), a local level committee constituted under the National Trust Act 1999? These are not drafting curiosities. They are the core design constraints of any Consent Manager operating under the Digital Personal Data Protection Act 2023 (DPDPA) and the Digital Personal Data Protection Rules 2025 (the Rules).

This article argues that the workable Consent Manager under the DPDPA is not a repository of consent receipts but a typed authority graph whose edges are bounded in time. Every time consent is captured, it is like a signed walk from the Data Fiduciary to the Data Principal along exactly one edge whose subtype is independently attested, independently bounded in time, and independently revocable. The possible subtypes track the statute, namely parent of the Data Principal, court appointed guardian, section 15 designated authority, National Trust local level committee, section 14 DPDPA nominee, Child Welfare Committee authorised representative, and Schedule IV Part A professional operating within a scope ring. Tokens issued by DigiLocker, by judicial registries, and by designated authorities form the issuance layer. Signed envelopes carrying consent payloads form the transport layer. The Graph is the element that unifies Rules 11's pluralism and the limited nature of carve-outs from Schedule IV into a unified capture regime instead of five.

This claim contains three elements, and each of them depends upon the statute. The first element is that Rule 11 does not regard guardian jurisdiction as a flag but rather a selection of three sources of truth, such as courts, Section 15 jurisdiction, and a local committee, all of which have their own registry and their own chain of evidence and revocation schedule. A consent architecture design that records merely the existence of a guardian without documenting the authority from which that status was derived cannot comply with the spirit of the regulation, even if it passes a tick-the-box audit. Thus, a consent architecture capable of fulfilling its purpose will recognize them as three entities. Moving to the second entity: the parent. The rules provide three methods of verifying the parent's consent in respect of his or her child, namely the use of pre-existing identity from the Data Fiduciary; the use of identity supplied by the user himself/herself in the process of giving the consent; and virtual token provided by a recognised authority like a Digital Locker. The mandate contained in section 9(1) of the statute

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

that the consent given shall be verifiable requires the method of verification to be recorded, and not reduced to an indistinguishable artefact. Third, look at the carve out. Five categories of Data Fiduciaries, specifically the clinical and mental health establishments, allied healthcare professionals, educational institutions, childcare establishments, and child transport providers, are provided relief from the rule mandating parental consent. However, this carve out does not relieve them of the restrictions imposed in sections 9(2) and 9(3). A consent architecture that tags Schedule IV status as a single Boolean cannot enforce that scope ring at all.

Recall that the Account Aggregator framework, for all its operational polish, was never asked to distinguish a court appointed guardian from a designated authority under a disability statute. Neither was it asked to encode a Child Welfare Committee order as per the Juvenile Justice Act 2015 as a bounded temporal authority processing mechanism. Consumer credit data is devoid of such authorities. Data relating to children, persons with disabilities, and Schedule IV are not. Thus, the Consent Manager, which is contemplated in section 6(7) of the DPDPA, carries with it an architectural problem the Account Aggregator does not have, and it can hardly be resolved through the extension of the Account Aggregator template alone.

Thus, there is a problem, both conceptual and architectural. The Board registered Consent Manager is meant to be the fiduciary intermediary prescribed by statute. As such, its architecture has to take into account the pluralism of authority and build in its complexity and not flatten it. Then, the five requirements enumerated in the fifth schedule of Schedule 1 Part B to the Rules, namely, opacity, retention, non-delegation, conflict avoidance, and fiduciary duty – will be built atop this system of capture as the cascade engine. These requirements are not addressed within the scope of this paper and, as such, the focus in what follows will be the capturing process.

The argument is made in five movements. Part II describes the problem arising from the pluralism of authority in Rule 11 and Schedule IV to the DPDPA. Part II will make clear why the architecture of the Consent Manager that relies on a Boolean, is_minor, has_guardian fails to distinguish the types of authorities recognized in the statute. It cannot because its failure to do so is, precisely, a compliance failure. Part III will describe the graph primitive. This will include identifying the node and edge taxonomy, the source-of-truth for each edge category, and the method of time bounding, scope rings, and revocation fields built into edges and not into the policy engine of the Consent Manager. Finally, a definition of the consent capture will be provided: a consent capture will be defined as a signed walk over exactly one authorizing edge. Part IV will position the consent capture graph with respect to the statute. It will describe the consents captures for: adult consents, children's verifiable parental consent under each of the three options under Rule 10, person-with-disability consents under each of the three options under Rule 11, and Schedule IV processing under Part A and B of said rule.

Part V explores two alternative primitives for consent capture, namely, the token-broker and the attestation envelope and makes the case against each as an alternative to the graph-based approach. Finally, Part VI addresses the decision maker under section 14 of RPwD, who, as is clear from Rule 11, is not considered as the lawful guardian of the person. Consequently, this decision maker must receive a reasoned refusal of consent, the logging of such denials becoming an evidentiary record of under-inclusion, one which the accompanying paper of this series will discuss thoroughly.

II. THE PLURALISM PROBLEM

II.A Rule 11's three guardian authorities and Schedule IV's scope restricted classes and purposes

Recall section 9(1) of the DPDPA mandates that a Data Fiduciary must first seek the consent from the parent/guardian before the processing of the data of any child/persons with disabilities who have a guardian as per the law. Rule 11 of the DPDP Rules 2025 does the job of informing the Data Fiduciary about the guardian in such a case, and Rule 11 identifies three such authorities. A guardian is lawful under Rule 11 if she has been appointed by a court of law, or by a designated authority under section 15 of the Rights of Persons with Disabilities Act 2016, or by a local level committee constituted under section 13 of the National Trust Act 1999.

Each of these signing authorities is embedded in its own statutory framework. The court appointment path takes one via civil procedure, usually by way of guardians and wards petition under the Guardians and Wards Act, 1890, and results in a guardianship order registered at the court registry. The section 15 path takes one via the district authority appointed under the RPwD Act in order to support the exercise by a person with disability of her legal capacity. The committee at the local level path takes one via a National Trust committee for each district, and involves the appointment of a guardian for persons having autism, cerebral palsy, mental retardation or multiple disabilities. Thus, a Data Fiduciary seeking to satisfy his obligations under rule 11, on account of performing due diligence, is actually making three checks, against three different registers, against three different signing authorities, and against three different rhythms of revocation. In addition to this plurality, Schedule IV offers even more complexity. Part A of Schedule IV identifies five categories of Data Fiduciaries whose processing activity in relation to personal data of the child is permitted without parental consent if restricted to the scope provided by the Schedule. A clinical establishment or mental health professional can process personal data of a child only to the extent required for protecting his health; an allied healthcare professional can process only to the extent necessary to implement a treatment

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

and referral plan. Educational institution can do so only to monitor the child's behaviour for its own educational purposes. A childcare provider can process only to ensure safety of the children entrusted with it; and a transport service catering to children can process only to monitor locations to ensure their safety while transporting them to and from the institution. These permissions to process are granted by five different regulators, viz., the National Medical Commission, the Rehabilitation Council of India, the National Council for Teacher Education, and the corresponding State level regulators for crèches and child transport. The list is not exhaustive. Part B of Schedule IV further limits permissions. Five exempt purposes are permitted under the Schedule: exercising powers conferred under Indian law for the welfare of children, providing subsidies or any other kind of public benefit, creating an email only user account, filtering detrimental access to information, and verifying age.

What we see is not a singular image of the "lawful consenter" but an intricate web of authorities. Rule 11 contributes three for people with disabilities. Schedule IV Part A provides five for child Data Fiduciaries. Schedule IV Part B provides five for exemptions. Section 14 of the DPDPA adds the nominee, who acts as the representative of the Data Principal in case of his/her demise or incapacitation. This means that a Data Fiduciary working under this law needs to have the capability of routing the consent capture process via any of these authorities, noting the chosen authority, and maintaining a record of the process in such a way that the latter can be independently re-verified in the future by a subsequent auditor, Board process, or court proceeding. The architecture supporting this will have to understand authority in its essence and not in terms of simple flags as this is neither a binary yes or no option. It will have to consider authority as a typed artifact with the type itself being part of the statutory process. The result of this is a record saying "This is a court-appointed guardian for education and medical care, issued on 5th March 2026 by the District Court at Pune under the Guardians and Wards Act of 1890, valid up to the ward turning eighteen."

II.B Why a Boolean flag collapses distinctions the statute treats as load bearing

Indeed, the data model reflects the theory, and the theory appears in the columns. In its simplest form, the temptation of the compliance department will appear as follows: the data principal's table contains two Boolean columns is_minor and has_guardian, plus one column with text for the guardian's identity and contact details. The data model is simple; it will validate easily; and it can be mapped directly onto the drop-down menu options of the onboarding form. However, it fails to comply with the statute at four different seams.

First, there is the issue of evidence. Rule 10 specifies three verification procedures for establishing parental consent for a child and, according to section 9(1), that consent must be verifiable. A Boolean field indicating only that the data principal is a minor cannot hold any information about the verification process. In a future audit, the auditor cannot determine whether the data fiduciary relied upon its own held record of identity (Rule 10(a)), a document provided by the user (Rule 10(b)(i)), or upon a token generated by a Digital Locker Service Provider (Rule 10(b)(ii)). The process used is a matter of fact that must be recorded by the data fiduciary and should not be left to implementation discretion. If that record is lost, so is the evidence produced by the Rule 10 process.

Secondly, there is the problem of authority plurality. According to Rule 11, three independent registries constitute acceptable sources of evidence of guardianship over individuals with disabilities. The three authorities have been granted identical legal power, and a Boolean has_guardian field cannot distinguish a court-appointed guardian from a registered one at the section 15 RPwD agency and from yet another who operates through a National Trust Local Level Committee. Each source implies a distinct procedure, registry, revocation protocol, and authority range. The data fiduciary seeking to re-verify the appointment will have to know which authority to address. An auditor verifying the chain of trust will have to know whose signature was on the attestation. The Boolean makes both tasks impossible.

The third seam is scope enforcement. Schedule IV Part A does not grant a general consent waiver to the five enumerated classes of Data Fiduciaries. It grants a waiver bounded by purpose. An architecture that flags a Data Fiduciary as a Schedule IV Part A class, without also binding the permitted purpose to the processing event itself, cannot prevent a childcare provider from using the carve out to justify engagement analytics or a school from using it to justify advertising targeted at its pupils. Section 9(3) forbids both. The Boolean abstracts away the exact variable the Schedule uses to discipline the carve out.

The fourth seam is under inclusiveness. Section 14 of the RPwD Act 2016 permits a person with disability to enter a joint decision making arrangement with a supporter of her own choice, without any court order and without any designation under section 15 of RPwD Act, 2016. Rule 11 of the Rules does not recognise this supporter as a lawful guardian. A Data Principal who has chosen a supporter under RPwD Act therefore has no pathway to verifiable consent under the Rule, even where the RPwD Act itself treats the arrangement as the paradigm case of supported decision making. A Boolean model cannot even make this gap visible, because it has no field for the attempted authority type that the Rule has declined to recognise. The gap becomes invisible, and with it the evidentiary record that a later reform process would need.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Hence the argument of this paper. Authority under the DPDPA is plural, and the design of the Consent Manager must be plural with it. Part III develops the primitive that carries this plurality, namely the typed authority graph, and shows how each of the four seams above is addressed not by a policy layer wrapped around the data model but by the data model itself.

III. THE GRAPH PRIMITIVE

III.A Nodes, typed edges, and sources of truth

What does a Consent Manager need to know in order to route a consent capture correctly? It needs to know who the Data Principal is. It needs to know who, if anyone, is lawfully authorised to consent on her behalf. And it needs to know where that authorisation came from, who signed it, and how long it remains good. A typed authority graph makes each of these facts a first class object. The nodes are the parties. The edges represent the authorities connecting the nodes. The type system of the graph represents the statute's classification of the entities capable of giving consent for others.

The scope of the vocabulary for nodes is not quite what it seems. A Data Principal node identifies the individual whose personal data will be processed. A natural person node is the adult individual in relation with the Principal node, usually a parent or nominee under section 14 DPDPA, a guardian nominated under civil law, or nominated by the National Trust Committee under section 13 National Trust Act. An institution node identifies a corporate or unincorporated establishment in three possible roles, namely as a Data Fiduciary, as a processor engaged by a Data Fiduciary, and as a licensed professional belonging to any of the classes specified in Schedule IV Part A. A Designated Authority node identifies the statutory position that confers or takes back the authority represented by an edge, for example, a civil court, a District authority nominated under section 15 of the RPwD Act, or a National Trust local level committee. Each node has an identifier, the unique number used by the statute to identify the individual or institution referred to, and a set of verified attributes.

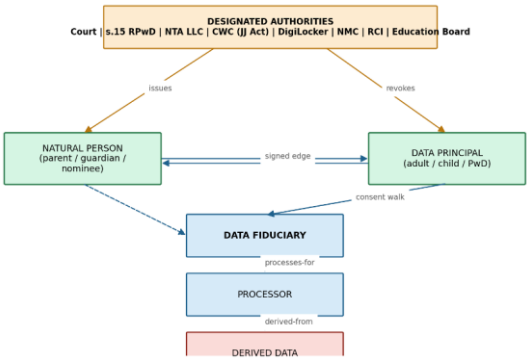

Figure 1. Node and edge topology, Source: Author.

The edges are responsible for the doctrinal underpinning of the model. Each edge has a type, a source node, a target node, an issuing authority, an attestation signature, a validity period, a scope descriptor, and a revocation hook. The type is taken from a closed set of vocabulary terms, tracking the statute.

The parental relationship between a natural person and the Data Principal who is his or her child has been denoted as parent-of, and has been issued based on one of the verification paths defined in Rule 10. When the identity of the parent can be confirmed based on an existing identity record maintained by the Data Fiduciary, the source of truth for the edge will be the KYC records maintained by the Data Fiduciary themselves, which can only be traced back to an authorized identity document. In case the identity of the parent can be obtained from the parent itself during the process of obtaining consent, the source of truth would be the document and its record maintained by the Data Fiduciary. The edge records which of the three paths was used.

The three guardian relations for a person with disability run parallel to one another. An edge labelled court-guardian-of is issued by a court registry and references the order number and the court of record. An edge labelled s15-designated-authority-for is issued by a district authority designated under section 15 of the RPwD Act and references the authority's order and jurisdictional scope. An edge labelled llc-guardian-of is issued by a local level committee constituted under section 13 of the National Trust Act and references the committee resolution. Each of the three carries a different signing key. Each references a different canonical registry. A Data Fiduciary receiving a consent along any of the three must verify against the correct registry for that edge type, and the graph makes the choice of registry a property of the edge rather than a private decision of the Data Fiduciary.

A nominee relation, labelled nominee-for, is issued under section 14 of the DPDPA and runs from a natural person to the Data Principal. The source of truth is the Data Fiduciary's own nominee register, which the Data Principal populates during her lifetime and which the Rules will in time require to be interoperable with other Data Fiduciaries. The edge is dormant until the triggering event, namely the Principal's death or declared incapacity.

A Child Welfare Committee relation, labelled cwc-authorised-for, is issued by a Committee constituted under section 27 of the Juvenile Justice Act 2015 and operates as a Schedule IV Part B Entry 1 authority. The edge references the Committee order, the specific child, and the specific purpose within the child welfare carve out. It is narrower than a parental edge and typically shorter lived.

A professional scope edge, labelled sch-IV-A-professional-for, sits differently from the others. It runs from an institutional node to a Data Principal node who is a child, and it does not authorise the institution to consent on the child's behalf. It authorises the institution to process the child's personal data without parental verifiable consent, provided the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

processing remains inside the scope ring the Schedule prescribes for that class. The source of truth is the professional's license, which is the NMC record of the clinics and mental health establishments, the RCI record of allied healthcare professionals, the Board of Education record of the educational institution, and the State-level record of crèches and child transport services. The scope field of the edge is mandatory; otherwise, it is an invalid edge.

The next two node relationships form the minimum set of edges required to represent the legal relations. The processing delegation relationship labelled processes-for is drawn from the processor node to the Data Fiduciary and is governed by the non-delegation discipline as per Schedule 1 Part B of the Rules. The data lineage relationship labelled derived-from connects the derived dataset to the consents underlying its input datasets. This edge structure forms the foundation of withdrawal cascades as per Section 6(4).

There are two characteristics of edges worth highlighting at this point. First, each edge is signed by the authority issuing the edge and not by the Data Fiduciary who relies upon that edge. The latter verifies the claim based on a public key of the former; the former does not issue claims. Second, each edge has an individual revocation hook embedded within it. A court revoking a guardianship, an authority modifying a designation, and a local body withdrawing a guardianship all send a signal to the graph using the respective revocation hook embedded in each edge. No polling of registers is required by the Data Fiduciary to check whether an edge has expired; the register makes the pronouncement.

III.B Time bounding, scope rings, and consent as a signed walk

An eternal authority is not an authority as understood by DPDPA. All edges in the graph are equipped with a validity interval, and the validity interval is a signed attribute of the edge rather than being policy bound. The valid_from attribute keeps track of the time when the edge was issued by the authority, and this comes from the issuing authority, such as the date of issue from the court order or the date from a local committee decision. The valid_until attribute tracks the end of the edge's life span. A parental edge issued under Rule 10 lapses when the child attains majority, and the graph computes the date from the date of birth captured at edge creation. A court guardianship edge lapses when the order says it lapses, typically on attainment of majority by the ward or on a date the court specifies, and the graph reads the instrument at creation and records the computed expiry. A National Trust local level committee edge lapses on the terms of the committee resolution. A Child Welfare Committee edge lapses with the duration of the specific order, and the graph refuses to treat it as a running authorisation beyond that window.

Scope rings do the work of bounding what an edge may authorise.

A scope ring is a tuple that sits alongside the validity window and that the graph engine consults at every processing event. For an edge of the parent type, the ring is wide, namely any processing consistent with the purpose set out in the section 5 notice and subject to the section 9 prohibitions on detrimental processing and tracking and targeted advertising. For an edge of the court guardian type, the ring is whatever the order itself prescribes, and where the order is silent, the ring defaults to the decisional domain that the Guardians and Wards Act 1890 treats as the guardian's ordinary remit. For an edge of the section 15 designated authority type, the ring is the domain set out in the designation instrument, which in most cases is narrower than a full guardianship. For an edge of the National Trust local level committee type, the ring tracks the LLC resolution. For a Schedule IV Part A professional edge, the ring is prescribed by the Schedule itself and is not negotiable by the Data Fiduciary, namely protection of the child's health for clinical and mental health establishments, implementation of a recommended treatment and referral plan for allied healthcare professionals, educational activities or safety of enrolled children for educational institutions, safety of children in care for childcare providers, and location tracking in the interests of safety for child transport services during travel. A processing event that falls outside the ring causes the graph to fail closed, without any further policy evaluation. The ring is where the Schedule's drafting becomes operational discipline.

Consent, in this model, is an event that the graph records as a signed walk. A walk begins at the Data Fiduciary node and ends at the Data Principal node. It traverses exactly one authorising edge. It bears the notice published in section 5 of DPDP Act, the purpose stated in that notice, the categories of data to which the walk pertains, and the validity period of the walk. It records the authorised edge traversed, including the type of the edge, the issuer of the edge, the validity window of the edge at the time of traversal, the scope ring of the edge, and the revocation hook of the edge. The document is signed by the Data Fiduciary in her official capacity of record-verifier, and is countersigned by the Consent Manager in his official capacity of ledger of walks. The free, informed consent obtained from the Data Principal or their guardian, documented using the user interface of the Data Fiduciary or Consent Manager, is the content of the walk.

There are two consequences of this definition that need to be spelled out clearly. First, every consent event is auditable by re-traversal. An auditor tasked with auditing the transaction, a Board conducting an investigation into a case, or a Court ordered to examine a consent can trace the relevant edge on the graph, verify the signatures against the key at issuance, verify the validity period and scope of the walk, and reconstruct the transaction based on these verified

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

components. This verification process is automatic because the recording format is well-structured, and the recording format is structured because the statute is plural. Second, revocation, too, is a walk. The withdrawal of consent from a parent under section 6(4), discharge of a child welfare direction by a Committee, or vacation of guardianship order by a Court each revokes the edge they issued directly, or indirectly derive from. The graph traces back from the revoked edge along all processes-for and derived-from edges that depend on the invalidated edge, and delivers revocation notices at each such node. The cascade of revocation is built into the graph topology.

One final point. The authority graph is not the Consent Manager itself. It is the primitive on which a Board registered Consent Manager must be built, if it is to carry the statute's own vocabulary. The issuance layer, namely the tokens minted by DigiLocker, by judicial registries, and by the three classes of disability authority, supplies the signed attestations that populate edges. The transport layer, namely the signed envelope that accompanies a consent across the Data Fiduciary's processing boundary, carries a single walk from capture to processor. The graph sits between them and makes the walk coherent, the edges re verifiable, and the scope rings enforceable. Part IV applies the primitive to each of the capture flows the DPDPA and the Rules contemplate.

IV. CAPTURE FLOWS

IV.A Adult consent and child verifiable parental consent under Rule 10

The simplest walk in the graph is the self-loop. An adult Data Principal consents for herself, without any intervening authority, and the graph records a walk from the Data Fiduciary node to the Data Principal node along an edge of type adult-self whose source of truth is the verification of adulthood the Data Fiduciary has itself performed. That verification may rest on Aadhaar offline KYC, on a passport or driving licence supplied at onboarding, or on any other identity instrument the Data Fiduciary is authorised to rely on under applicable Indian law. The edge carries no guardian, and the scope ring is the purpose set out in the section 5 notice. A processing event outside that purpose is an event the graph will refuse to authorise, because the scope ring does not accommodate it. The adult self-loop is the base case against which every other flow stands as a variation.

The first variation the statute demands is for a child. Section 9(1) of the DPDPA requires a Data Fiduciary, before processing the personal data of a child, to obtain verifiable consent of the parent in such manner as may be prescribed. Rule 10 of the Rules prescribes the manner. It obliges the Data Fiduciary to adopt appropriate technical and organisational measures, and to observe due diligence for checking that the individual identifying herself as the parent is an adult who is identifiable, where such identification is required in connection with compliance with any law for the time being in force. The Rule offers three paths for this identification, and each path instantiates a parent-of edge in the graph with a different source of truth.

The first path, in Rule 10(1)(a), uses reliable details of identity and age of the individual already available with the Data Fiduciary. Consider a bank that already holds a customer's KYC documentation, and that is now asked to process the personal data of that customer's minor child for the opening of a minor operated account. The bank runs the parental consent flow against its own held identity record, finds that the parent is an adult as identified by her Aadhaar or passport captured at onboarding, and issues a parent-of edge from her node to the child's node. The edge's source of truth is the bank's own verified KYC record. The graph stores a reference to that record and a date stamp recording when the check was performed. A later audit against Rule 10(1)(a) is mechanical. The auditor traverses the edge, reads the reference, verifies that the KYC record exists and was valid on the date stamped, and reads the signature of the bank as verifier of record.

The second path, in Rule 10(1)(b)(i), uses details of identity and age voluntarily provided by the individual at the point of consent. Consider a consumer application that does not hold a prior KYC for the parent, and that asks the parent to upload a government identity document at the moment of the child's data processing request. The application verifies the document, confirms adulthood, and issues a parent-of edge. The edge's source of truth is the document presented and the application's own verification log, including the cryptographic hash of the document and the result of any optical character recognition and database lookup performed. The Rule does not require the Data Fiduciary to retain the document itself beyond the verification window, but the graph does require the Data Fiduciary to retain the verification record, namely the hash, the lookup result, and the date. The edge records which sub path was used, namely (b)(i), and the audit proceeds accordingly.

The third path, in Rule 10(1)(b)(ii), uses a virtual token mapped to the parent's identity and age, issued by an authorised entity. The Rule defines an authorised entity is any entity designated by law, or by the Central or State Government for the issuance of any identity and age details or a virtual token mapped to such details and also any Digital Locker Service Provider. Suppose there exists an educational technology platform that has received a DigiLocker issued age attestation token based on a mapping from the parent's Aadhaar or PAN number. In that case, the authentication will be carried out using DigiLocker as the parent has issued an attestation token confirming his or her adulthood status and also showing that the parent is related to the child based on the family relationship records available with the Digital Locker Authority. There is no receipt of any of the personal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

information of the parent, which may include the Aadhaar or the PAN number. What is being verifiedan authorised entity is any entity designated by law, or by the Central or State Government for the issuance of any identity and age details or a virtual token mapped to such details and also any Digital Locker Service Provider. Suppose there exists an educational technology platform that has received a DigiLocker issued age attestation token based on a mapping from the parent's Aadhaar or PAN number. In that case, the authentication will be carried out using DigiLocker as the parent has issued an attestation token confirming his or her adulthood status and also showing that the parent is related to the child based on the family relationship records available with the Digital Locker Authority. There is no receipt of any of the personal information of the parent, which may include the Aadhaar or the PAN number. What is being verified is the signed token sent over by the parent. After successful validation of the token based on the DigiLocker's public key, confirmation of the validity window, and the generation of a token, a parent-of edge will be generated, whose source of truth is the token itself. The type of sub path used in the process will be recorded, as well as the token identifier, its issuer, and date of verification of the token.

Three characteristics stand out with regards to the child capture flow process. First, the three paths do not exist in hierarchical relationships with each other. For instance, the Rule does not require a Data Fiduciary to exhaust path (a) before opting to use path (b). Instead, the Rule allows the Data Fiduciary to opt for the method that would fit in the best given its operational environment. This implies that in the Graph, the source of truth is the sub path selected and its subsequent recording in order to meet the requirements of the Rule. Second, the three paths produce parent edges which differ in their evidentiary value. The nature of the evidence backing the edge when the source of truth is either one of the two paths will be different from that in the third path which involves the virtual token attestation. Thus, the Graph maintains the distinction by having the source of truth as a structural aspect in the edge. The Data Fiduciary's auditors, at some future time, will develop an auditing strategy based on the evidentiary strength of the edge. Third, the adulthood attestation is a limited claim on the part of the Data Fiduciary. is the signed token sent over by the parent. After successful validation of the token based on the DigiLocker's public key, confirmation of the validity window, and the generation of a token, a parent-of edge will be generated, whose source of truth is the token itself. The type of sub path used in the process will be recorded, as well as the token identifier, its issuer, and date of verification of the token.

Three characteristics stand out with regards to the child capture flow process. First, the three paths do not exist in hierarchical relationships with each other. For instance, the Rule does not require a Data Fiduciary to exhaust path (a) before opting to use path (b). Instead, the Rule allows the Data Fiduciary to opt for the method that would fit in the best given its operational environment. This implies that in the Graph, the source of truth is the sub path selected and its subsequent recording in order to meet the requirements of the Rule. Second, the three paths produce parent edges which differ in their evidentiary value. The nature of the evidence backing the edge when the source of truth is either one of the two paths will be different from that in the third path which involves the virtual token attestation. Thus, the Graph maintains the distinction by having the source of truth as a structural aspect in the edge. The Data Fiduciary's auditors, at some future time, will develop an auditing strategy based on the evidentiary strength of the edge. Third, the adulthood attestation is a limited claim on the part of the Data Fiduciary. The graph records the band rather than the age, and the Data Fiduciary's data minimisation obligation under section 6(1) and the Schedule 1 Part B opacity obligation are both honoured as a consequence of the edge schema.

One further point that the flow makes visible. Recall that section 9(2) forbids processing likely to cause a detrimental effect on the well-being of a child, and section 9(3) forbids tracking, behavioural monitoring, and targeted advertising directed at children. A parent-of edge authorises processing of the child's personal data, but it does not authorise processing that breaches either sub section. The scope ring carried by the edge inherits the section 9(2) and section 9(3) prohibitions as hard constraints on the Data Fiduciary's processing events, and the graph engine refuses to authorise an event that triggers either. A parent cannot, under the DPDPA, consent the child into a form of processing the statute itself forbids, and the graph reflects the prohibition rather than leaving it to the Data Fiduciary's own policy layer.

IV.B Person with disability consent under Rule 11

The second variation on the adult self-loop is for a person with disability who has a lawful guardian. Section 9(1) of the DPDPA treats this Principal in parallel with a child, and requires the Data Fiduciary, before processing her personal data, to obtain verifiable consent of her lawful guardian in such manner as may be prescribed. Rule 11 of the Rules prescribes the manner, and it does so in the disjunctive. The Data Fiduciary must observe due diligence to verify that the self-identifying guardian has been appointed by a court of law, or by a designated authority under section 15 of the Rights of Persons with Disabilities Act 2016, or by a local level committee under section 13 of the National Trust Act 1999. The three authorities are equal in legal standing, and a Data Fiduciary is compliant if it verifies the appointment under whichever route the guardian in fact holds. The graph instantiates each of the three as its own edge subtype, so that the route the Data Fiduciary verified is itself a recorded fact.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The first route is the court appointed guardian. Consider an adult Data Principal who, following a civil proceeding under the Guardians and Wards Act 1890, has had a guardian appointed by a district court. The court has issued an order naming the guardian, recording the scope of her authority, and, in most cases, setting the duration of the appointment or the conditions on which it ends. The graph instantiates a court-guardian-of edge from the guardian to the Principal. The edge's source of truth is the court registry's record of the order, retrievable by the case number and bench. The edge's scope ring is the scope the order itself prescribes, or where the order is silent, the default remit that the 1890 Act allocates to a guardian of the person or of the property as the case may be. The edge's validity window runs from the date of the order to the date the order specifies, or to the date on which the ward attains majority where the guardianship is of a child. A Data Fiduciary verifying this edge at the point of consent capture resolves the order against the court registry, confirms that the order is live and not vacated or modified, and proceeds to record the walk. The audit artefact is the registry lookup record, signed and time stamped, and travelling with the walk in the signed envelope.

The second route is the section 15 RPwD Act designated authority. Recall that section 14 of the RPwD Act 2016 addresses legal capacity and supported decision making, and section 15 provides for the designation of an authority in each district to support persons with disability in the exercise of their legal capacity. A guardian appointed by a section 15 authority operates within a statutory frame that is lighter touch than a court guardianship, and the RPwD Act expressly treats the arrangement as support rather than substitution. The graph instantiates an s15-designated-authority-for edge from the appointed person to the Data Principal. The edge's source of truth is the district authority's register of appointments, which the notification designating the authority under section 15 will in time require to be publicly verifiable. The edge's scope ring is the domain set out in the designation instrument, which in most cases is narrower than a full guardianship and may for instance be limited to decisions concerning health and welfare or to decisions concerning financial affairs. The edge's validity window runs from the designation to its lapse or revocation, each of which the authority records. A Data Fiduciary verifying this edge resolves the reference against the authority's register and confirms that the appointment is live and that the proposed processing falls within the designated domain. A processing event that lies outside the domain fails closed, because the scope ring does not cover it.

The third route is the National Trust Act local level committee. Section 13 of the NTA, 1999 Act constitutes a committee in each local area, under section 14 of that Act, with power to appoint a guardian for a person with autism, cerebral palsy, mental retardation, or multiple disability. The committee's appointment produces a written resolution specifying the guardian and, in most cases, the scope of her authority. The graph instantiates an llc-guardian-of edge whose source of truth is the committee resolution in the local committee's register, and whose scope ring tracks the resolution. A Data Fiduciary verifying this edge consults the committee's register, confirms the resolution is un-rescinded, and records the walk. The three routes are architecturally parallel, but each speaks to a different statutory frame, and the graph preserves the difference because the statute itself treats the frames as distinct.

Two points must be noticed here, and each supplies the bridge to Part VI. The first is that Rule 11's disjunctive is closed. A guardian who has not been appointed along one of the three named routes is not, for the purpose of Rule 11, a lawful guardian. An adult child of an ageing parent, whose parent has informally delegated decisions to her under a consensual family arrangement, is not a lawful guardian under Rule 11 unless the arrangement has been ratified by a court, a section 15 authority, or a local level committee. The graph cannot issue a parent-of edge for an adult Principal, because the Principal is not a child, and it cannot issue any of the three Rule 11 edge subtypes, because none has been conferred. The consent flow therefore fails closed, and the graph records the attempted walk with a reason code drawn from the statute.

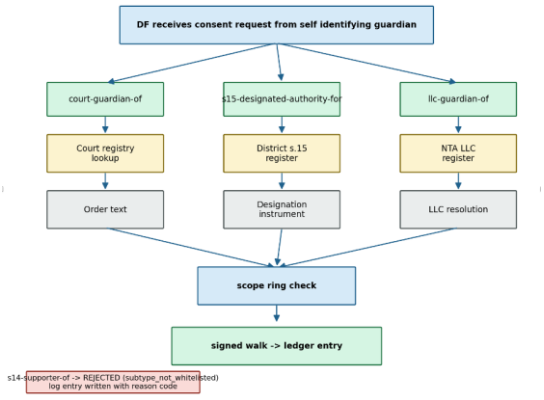

Figure 2. Person with Disability consent walk with three parallels under Rule 11. Source: Author

The second point concerns the section 14 RPwD Act supporter. Section 14 recognises a supported decision making arrangement entered into by the Principal of her own volition with a person of her own choice, and does not itself require court appointment or section 15 designation. Rule 11 does not recognise this supporter as a lawful guardian. A Data Fiduciary presented with a supporter who produces documentation of a section 14 arrangement cannot route the consent along it, because the Rule's list of authorities is closed. The graph records the attempt, names the edge subtype requested, and returns a reason code that the Rule does not whitelist the subtype. Part VI takes up the evidentiary use of this log. The capture side of the paper stops at recording the rejection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

IV.C Schedule IV Parts A and B

Schedule IV of the DPDPA does not authorise a third party to consent on behalf of a child. It does something different. Part A carves out five classes of Data Fiduciaries whose processing of a child's personal data is permitted without verifiable parental consent, provided the processing remains inside a scope ring the Schedule itself prescribes. Part B carves out five exempt purposes along similar lines. Neither Part treats the carve out as a general waiver. Each treats it as a narrow permission, bounded by the class or the purpose, and the graph must encode the boundedness at the level of the edge rather than at the level of policy wrapped around a flag.

The Part A carve outs produce edges of an institutional kind. Consider an urban multi-speciality hospital receiving a child brought in for treatment by a parent, where the parent has not executed a consent artefact through a Consent Manager and where the hospital must process the child's personal data to render care. The hospital falls within Entry 1 of Part A as a clinical establishment. The graph instantiates a sch-IV-A-professional-for edge from the hospital node to the child's node, with the class attribute set to clinical establishment and the scope ring set to the text the Schedule prescribes, namely provision of health services to the child to the extent necessary for the protection of her health. The edge's source of truth is the hospital's registration under the Clinical Establishments (Registration and Regulation) Act 2010 and the underlying licence issued under the relevant State law. The edge's validity window tracks the currency of that registration. A processing event by the hospital that sits inside the scope ring, such as recording the child's diagnosis, ordering an investigation, and communicating with the treating paediatrician, is authorised by the edge. A processing event outside the ring, such as sharing the child's health data with a pharmaceutical sponsor for market research, is not. The graph refuses it closed, and the refusal is a property of the edge's scope rather than a discretionary exercise of the hospital's compliance team.

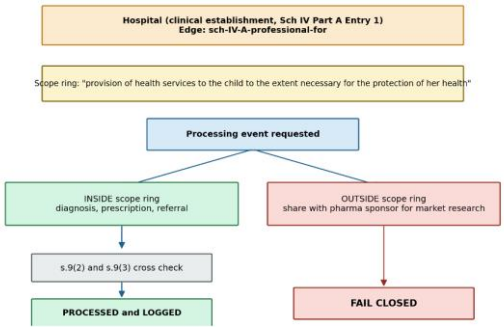

Figure 3. Schedule IV Part A scope ring enforcement. Source: Author

The remaining four Part A classes instantiate edges of the same shape but with different scope rings. An allied healthcare professional registered with the Rehabilitation Council of India, a nutritionist, a physiotherapist, or a speech therapist, for instance, receives an edge whose scope ring tracks the implementation of a recommended treatment and referral plan to the extent necessary for protection of the child's health. An educational institution recognised by the appropriate Board receives an edge whose scope ring covers tracking and behavioural monitoring for the institution's own educational activities and for the safety of enrolled children, and nothing further. A childcare provider operating a crèche or daycare receives an edge whose scope ring is bounded to safety of the children in its care. A child transport service receives an edge whose scope ring covers tracking the location of children during travel to and from the institution or crèche. In each case, the scope ring is the text the Schedule prescribes. A processing event outside the ring is not authorised, and the graph enforces the boundary at the processing layer rather than the consent layer.

Two cross cutting prohibitions ride above all five Part A edges. Section 9(2) forbids processing likely to cause a detrimental effect on the well being of a child, and section 9(3) forbids tracking, behavioural monitoring, and targeted advertising directed at children. Part A dispenses with the consent requirement but does not dispense with these prohibitions. An educational institution relying on the Entry 3 carve out may track the attendance and academic progress of its pupils, but it may not extend that tracking to behavioural profiles fed into an advertising network. A childcare provider may monitor the safety of a child in its care, but it may not share the resulting data with a sponsor seeking to target parents for commercial products. The graph carries the section 9(2) and section 9(3) constraints as hard rules at the processing layer, applied regardless of edge type. A processing event that satisfies the scope ring of a Part A edge but triggers either sub section fails closed, and the refusal is recorded.

Part B exempts five purposes rather than five classes of Data Fiduciary. Each purpose is narrow, each rides on its own authority, and each instantiates a purpose scoped edge in the graph. A Child Welfare Committee acting under section 27 of the Juvenile Justice (Care and Protection of Children) Act 2015, in exercise of the powers Entry 1 of Part B preserves, issues a cwc-authorised-for edge authorising processing in the interests of the specific child named in the Committee's order, for the specific purpose the order identifies, and for the duration the order sets. A sanctioning ministry or State department distributing a subsidy or a benefit under a public scheme issues a statutory-benefit-for edge authorising processing to the extent necessary for conferring the subsidy, benefit, service, certificate, licence, or permit contemplated by Entry 2. A platform creating an email only account for a child under Entry 3 issues a sch-IV-B-email-account-for edge whose scope ring is limited to the operation of that account. A platform operating content filtering under Entry 4 issues an edge whose scope ring is limited to the prevention of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

detrimental information access. A platform performing age verification under Entry 5 issues an edge whose scope ring is limited to the confirmation of age or observance of due diligence. In each case the authority is external to the Data Fiduciary. In each case the scope is prescribed and non negotiable. In each case the graph carries the authority and the scope together, so that the audit and the processing layer both have the material they need.

The cumulative effect of Parts A and B in the graph is a population of authorising edges of different shapes and different rings, each issued by a different source of truth. A Data Fiduciary subject to the DPDPA and the Rules must be able to route a consent or a processing authorisation along any one of them, record which one was used, and honour the scope ring that came with it. The graph is, in that sense, the statute's own diagram rendered as a data model.

V. WHY NOT TOKENS ALONE, WHY NOT ENVELOPES ALONE

Two architectural primitives rival the typed authority graph as candidates for a Board registered Consent Manager, and each deserves a short examination. The first is the token broker, in which a central Consent Manager routes signed tokens minted at the issuing authorities and carries no substantive authority record of its own. The second is the attestation envelope, in which each consent artefact is a self-contained signed package, and the Consent Manager functions as an immutable ledger of envelopes while the Data Fiduciary verifies each envelope on receipt. Each of these primitives does useful work. Neither, taken alone, carries the doctrinal load the statute places on the capture layer.

The token broker architecture is attractive because Rule 10(1)(b)(ii) itself points toward it. The Rule recognises a virtual token issued by an authorised entity as a verification path, and names the Digital Locker service provider as an included example. A design that concentrates authority and identity on the issuers, and the Consent Manager only serves as a transfer layer to move the signed tokens between the parties, ensures that the Consent Manager remains lightweight and there is no need for creating a central repository for identity. It is indeed useful. However, the problem is that the token is an atomic artefact. It verifies the identity of one individual at one time for one purpose – usually, for being an adult or having a certain title. In itself, the token does not provide the relational structure required by the statute. Rule 11's three authorities are not three tokens of the same kind. They are three sources of truth with different scopes, different registries, and different revocation protocols. A token broker that transfers tokens but fails to classify the tokens makes the Data Fiduciary responsible for classifying them on receipt and making the auditors do the same. The typed artefact is either part of the architecture or recreated by every user who works with it.

The attestation envelope architecture addresses a completely different issue. Its underlying concept is that the evidentiary process should remain within the consent artefact itself, allowing the Data Fiduciary to check the envelope independently without contacting a centralized authority after each processing activity. Such envelopes can now be adequately represented by current standard architectures such as the Remote Attestation Procedures Architecture, defined in RFC 9334, and the Verifiable Credentials Data Model 2.0, published by the World Wide Web Consortium. Both models possess numerous advantages. For example, the envelope requires the issuing authority to verify its claim using a cryptographic signature. It allows the Data Fiduciary to carry the proof with the artefact so that other parties, including processors, can confirm without communicating with the Consent Manager again. Furthermore, it creates an audit trail that can be reviewed by courts without having access to the records of the Consent Manager. However, the drawback is that an envelope can only contain proof of a successful consent collection process at a particular moment. It cannot reflect any changes made in the original source of authority, e.g., when the court modifies the guardianship order or when the disability designation gets updated, or when the local level committee changes the scope of its resolution. The envelope only reflects the state of affairs at the time of issuance; it does not refer to the authority behind it.

In contrast, the typed authority graph sits atop the two primitives and does what neither can do alone. It represents the relationship between the parties as a first-class artefact. Unlike a token or an envelope, a court-guardian-of edge is neither the signed token verifying the guardian's appointment on the issuance day nor the envelope reflecting that appointment. Instead, it is the edge itself, containing a validity period, scope ring, and revocation hook. Each of those artefacts can change depending on new orders, revisions, or resolutions made by the authorities concerned. A token captures a moment, while an envelope captures a journey. However, the authority graph captures authority across all moments and all journeys. It is the only structure capable of supporting the longitudinal approach required by the statute, i.e., verifying authority at each processing event and passing revocation cascades from upstream authorities into downstream artefacts.

The right way to read the three primitives is as a stack rather than as a contest. Tokens issued by DigiLocker, by judicial registries, and by the three classes of disability authority populate the graph's edges at creation. The graph types, bounds, and revises those edges across time. Envelopes carry individual walks across the Data Fiduciary's processing boundary, so that every processor and every recipient of a dataset can verify that the walk was authorised at the moment it was taken. Each primitive does what it does best, and the capture architecture works because all three are present. A

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Board registered Consent Manager that adopts tokens without the graph loses Rule 11's pluralism. One that adopts envelopes without the graph loses the longitudinal discipline the statute's revocation cascade requires. The graph is the primitive that holds the stack together, and neither of the rival primitives is, on its own, a substitute for it.

VI. THE SECTION 14 RPWD GAP AS A LOGGED REJECTION ARTEFACT

Section 14 of the Rights of Persons with Disabilities Act 2016 sits at the heart of the Act's theory of legal capacity. Section 13(2) affirms that persons with disability have legal capacity equally with others in all aspects of life. Section 14 then provides for supported decision making, under which a person with disability may enter an arrangement with one or more persons of her own choice to support her in the exercise of her legal capacity. The arrangement does not require a court order. It does not require a section 15 designation. It is consensual, self-initiated, and revocable at the will of the Principal herself. The RPwD Act treats this arrangement as the paradigm case of support, consistent with Article 12 of the United Nations Convention on the Rights of Persons with Disabilities, to which India is a party. Section 14 is the Act's expression of the move away from substituted decision making and toward an architecture of support.

Rule 11 of the DPDP Rules 2025 does not recognise a section 14 supporter as a lawful guardian for the purpose of section 9(1) of the DPDPA. The Rule names three authorities in the disjunctive, namely court appointment, section 15 designation, and National Trust local level committee appointment, and it names no fourth. A Data Fiduciary presented with a person with disability who wishes to consent through her section 14 supporter, rather than through a substituted decision maker appointed by one of the three listed routes, has no path through Rule 11 to a lawful capture. The Principal may, of course, consent for herself as an adult, which is the stance the RPwD Act itself prefers. But where the Principal has entered a section 14 arrangement precisely because she requires support to exercise her legal capacity, the Rule leaves her and her Data Fiduciary with no compliant pathway short of a conversion of the arrangement into a court appointment or a section 15 designation, each of which is heavier in evidentiary demand and in paternalistic cast than section 14 itself intends.

The graph does not fix this gap. It makes the gap visible and countable. The capture flow for a person with disability begins with the Data Fiduciary's query for an authorising edge, and the query is typed. A Data Fiduciary that receives a self-declaration of a section 14 arrangement, and attempts to create an edge of that subtype, places a candidate edge of type s14-supporter-of into the graph's creation path. The graph's edge type registry, which is closed to the Rule 11 disjunctive plus the Schedule IV edge types, returns a reason code that the subtype is not recognised. The attempted edge is not issued. The walk does not commence. The Data Principal receives a reasoned refusal, and the Data Fiduciary's audit log carries a structured entry, namely the date of the attempt, the identifier of the Data Principal node in pseudonymous form, the edge subtype requested, the claim of support arrangement under section 14 of the RPwD Act that the Data Principal asserted, and the reason code indicating that Rule 11 does not whitelist the subtype.

The log that results is a statutory artefact. Each entry is a refusal, but in aggregate the entries form an evidentiary record of how often, in which sectors, and at what scale the existing Rule 11 disjunctive forecloses access for persons with disability who have chosen a section 14 arrangement. A Data Fiduciary in the healthcare sector will in time have one such log. A Data Fiduciary in the financial sector will have another. The Board is empowered under section 27 of the DPDPA to call for such logs in the course of its functions. A later reform process, whether by MeitY, by the Board, or by a parliamentary standing committee, can draw on the aggregated logs to demonstrate the scale of the gap in empirical terms. The architecture does not advocate. The architecture records. The advocacy is the work of the literature that the records support.

The scope of this paper stops there. The question whether Rule 11 ought to be amended to recognise section 14 supporters as a fourth category of lawful guardian for the purpose of section 9(1) of the DPDPA is a normative question about the proper relationship between the RPwD Act and the DPDPA, and about the residual role of substituted decision making under Indian privacy law. The question engages Article 12 of the UN Convention, the Parliamentary Standing Committee's own treatment of disability and decisional autonomy, and the under inclusiveness critique that has been developed in the Indian disability rights scholarship. A companion paper in the author's research develops these arguments in full. For present purposes, the significance of the gap is architectural. The graph surfaces it, the log records it, and the later argument for reform has a countable record on which to rest.

VII. CONCLUSION

The tension with which this paper began is a tension internal to the DPDPA itself. The statute requires the Data Fiduciary to obtain verifiable consent of the parent or the lawful guardian before processing the personal data of a child or a person with disability, and it leaves the identification of that parent or guardian to a body of Rules and a Schedule that name, between them, a plurality of authorities of different kinds. Rule 10 offers three verification paths for a parent. Rule 11 offers three authorities for a guardian. Schedule IV Part A names five scope restricted classes of Data Fiduciaries, and Schedule IV Part B names five exempt purposes, each

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

riding on its own source of authority. The capture architecture that sustains this plurality must hold each of these authorities in a form that preserves what the statute treats as load bearing, namely the type of the authority, the source of truth that issued it, the scope within which it operates, and the window in which it remains good. A capture architecture that does less fails the statute at exactly the seams it was written to discipline.

The resolution this paper has developed is a typed authority graph, bounded in time and signed at the edge. Every consent capture is a signed walk from the Data Fiduciary to the Data Principal along exactly one authorising edge, whose subtype is one of those the statute recognises and whose source of truth is the issuing authority that statute names. Parts II through IV have shown how the primitive encodes Rule 11's pluralism, Rule 10's three verification paths, and Schedule IV's scope restricted carve outs, each as a distinct edge type with its own source of truth and its own scope ring. Part V has considered two rival primitives, namely the token broker and the attestation envelope, and has shown that each does useful work as a layer of the architecture but that neither, taken alone, carries the longitudinal discipline the statute requires. Part VI has traced a structural gap in Rule 11's closed list of guardian authorities, namely the absence of the section 14 RPwD supporter, and has shown how the graph surfaces the gap as a logged refusal rather than absorbing it invisibly.

Two consequences of the argument deserve naming in closing. The first is doctrinal. The Board registered Consent Manager contemplated by section 6(7) of the DPDPA is, on the account this paper has defended, the statute's chosen fiduciary intermediary, and its architecture must match the statute's pluralism of authority rather than smooth it away. The graph is not an implementation choice that sits beneath the law. It is the minimum form the law itself demands, made visible as a data model. The second consequence is architectural. The capture side of the Consent Manager is one half of what the statute asks the intermediary to do. The other half is the downstream discipline of processing, namely the opacity, retention, non-delegation, conflict avoidance, and fiduciary duty obligations that Schedule 1 Part B to the Rules places on the Consent Manager itself. Those obligations sit downstream of the capture graph, and they operate as the engine through which withdrawal under section 6(4) cascades from the Data Principal through the Data Fiduciary and onward to processors and derived data. The future research should argues that Schedule 1 Part B is best read as the specification of that cascade engine, and develops the five primitives on which the engine must be built. The capture graph and the cascade engine together constitute the workable Consent Manager under the DPDPA. This paper has set out the first.

REFERENCE:

[1] Vrinda Bhandari and Renuka Sane, "Towards a Privacy Framework for India in the Age of the Internet," NIPFP Working Paper No. 179 (Nov. 2016). SSRN No. 2892368.

[2] Vrinda Bhandari, Rishab Bailey, Smriti Parsheera, and Faiza Rahman, "Comments on the (Draft) Personal Data Protection Bill, 2019," SSRN No. 4051127 (Mar. 2021).

[3] Rishab Bailey, Smriti Parsheera, Faiza Rahman, and Renuka Sane, "Disclosures in Privacy Policies: Does 'Notice and Consent' Work?," NIPFP Working Paper No. 246 (Dec. 2018). SSRN No. 3328289.

[4] Vrinda Bhandari, Rishab Bailey, and Trishee Goyal, "Analysing India's KYC Framework through the Privacy Lens," SSRN No. 4093454 (Apr. 2022).

[5] Smriti Parsheera, Ajay Shah, and Avirup Bose, "Competition Issues in India's Online Economy," NIPFP Working Paper No. 194 (Mar. 2017). SSRN No. 3045810.

[6] Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins India, 2018).

[7] Rahul Matthan, "Consent-to-Port," Ex Machina (Substack), Sept. 9, 2020.

[8] Jack M. Balkin, "Information Fiduciaries and the First Amendment," 49 UC Davis Law Review 1183 (2016).

[9] Jack M. Balkin, "The Fiduciary Model of Privacy," 134 Harvard Law Review Forum 11 (2020).

[10] Smriti Parsheera, "Finding a Place for Privacy in India's Health Digitization Landscape," Center for the Advanced Study of India, University of Pennsylvania (2023).