बिहार सरकार

<u>स्वास्थ्य विभाग</u>

आदेश

पत्रांक-SHSB/DOSA/174/2025 /पटना, दिनांक-

UIDAI, नई दिल्ली का पत्रांक-HQ-13082/3/2023-AUTH-II HQ/C-12949/1563, दिनांक-22.05.2025 एवं सूचना प्रावैधिकी विभाग, बिहार सरकार के पत्रांक-1058, दिनांक 02.06.2025 के माध्यम से स्वास्थ्य विभाग, बिहार सरकार को सूचना प्रावैधिकी विभाग, बिहार सरकार (AUA/KUA) के Sub-AUA/Sub-KUA के रूप में Appoint किया गया है। Aadhar Act, 2016 एवं UIDAI द्वारा समय समय पर निर्गत दिशा-निर्देश के अनुसार स्वास्थ्य विभाग, बिहार सरकार अन्तर्गत Aadhar Authenticated गतिविधि / भुगतान के संदर्भ में Information Security Policy (Aadhar Authentication) 2025-26 Version 1.0 निर्गत किया जाता है।

यह Policy तत्काल प्रभाव से लागू किया जाता है।

ह०/-
(लोकेश कुमार सिंह)
सचिव

ज्ञापांक- SHSB/DOSA/174/2025..1112(12)...........स्वा०/पटना दिनांक-14/8/2025

प्रतिलिपिः अपर मुख्य सचिव, स्वास्थ्य-सह-मुख्य कार्यपालक पदाधिकारी, राज्य स्वास्थ्य समिति, बिहार को कृपया सूचनार्थ प्रेषित।

प्रतिलिपिः सचिव, सूचना प्रावैधिकी विभाग, बिहार सरकार पटना को सूचनार्थ एवं आवश्यक करवाई हेतु प्रेषित| Information Security Policy (Aadhar Authentication) 2025-26 Version1.0 पर अपना सुझाव देना चाहेंगे ताकि प्राप्त सुझाव के साथ Revised Information Security Policy (Aadhar Authentication) 2025-26 Version 1.0 निर्गत किया जा सके|

प्रतिलिपिः कार्यपालक निदेशक, राज्य स्वास्थ्य समिति, बिहार, पटना को सूचनार्थ एवं आवश्यक कार्रवाई हेतु प्रेषित।

प्रतिलिपिः प्रबंध निदेशक, बी०एम०एस०आई०सी०एल०, पटना को सूचनार्थ एवं आवश्यक कार्रवाई हेतु प्रेषित।

प्रतिलिपिः मुख्य कार्यपालक पदाधिकारी, बिहार स्वास्थ्य सुरक्षा समिति, बिहार, पटना को सूचनार्थ एवं आवश्यक कार्रवाई हेतु प्रेषित।

प्रतिलिपिः उप निदेशक,UIDAI, नई दिल्ली को सूचनार्थ एवं आवश्यक करवाई हेतु प्रेषित ।

प्रतिलिपिः सभी असैनिक शल्य चिकित्सक-सह-मुख्य चिकित्सा पदाधिकारी, बिहार को सूचनार्थ एवं आवश्यक कार्रवाई हेतु प्रेषित।

प्रतिलिपिः-निदेशक, CDAC, बिस्कोमान टावर, पटना को सूचनार्थ एवं आवश्यक कार्रवाई हेतु प्रेषित।

प्रतिलिपिः कार्यपालक निदेशक, राज्य आयुष समिति, बिहार को सूचनार्थ एवं आवश्यक कार्रवाई हेतु प्रेषित।

प्रतिलिपिः सभी प्रशाखा पदाधिकारी, स्वास्थ्य विभाग, बिहार, पटना को सूचनार्थ प्रेषित।

सचिव
14/8/2025

स्वास्थ्य विभाग
बिहार सरकार

Information Security Policy

(Aadhaar Authentication)

2025-26

Version 1.0

Information Security Policy and Procedure (Aadhaar Authentication)

Table of Contents

Scope

This is with reference to the Aadhaar Authentication Services of Unique Identification Authority of India (UIDAI) for the scheme namely

1. Janani Suraksha Yojana
2. Payment of Performance Based Incentives to Accredited Social Health Activists (ASHA) under National Health Mission
3. Payment of Remuneration to Contractual Staff engaged under National Health Mission
4. Revised National Tuberculosis Control Programme (RNTCP)
5. Family Planning Schemes under National Health Mission (5 Schemes)

   5.1 Enhanced Compensation Scheme for Sterilization for beneficiaries and service provider;

   5.2 Post-Partum IUCD (PPIUCD) Incentive Scheme to beneficiaries and service providers;

   5.3 Post-Abortion IUCD (PAIUCD) Incentive Scheme to beneficiaries and service providers;

   5.4 Ensuring Spacing of Births (ESB) Scheme

   5.5 Family Planning Indemnity Scheme (FPIS)
6. Other Schemes notified by Govt. of India / Govt. of Bihar, in which Aadhaar Authentication is required.

This document details the Information Security Policy and procedures applicable to Health Department, Govt. of Bihar and associated organizations, including State Health Society, Bihar (SHSB) as a Sub-Authentication User Agency (Sub AUA) / Sub e-KYC User Agency (Sub – KUA).

Document distribution

All Employees of Health Department, Govt. of Bihar and associated organizations including State health society, Bihar (SHSB) and third parties who access information through information system or handle any information Asset of SHS, Health Department, Govt. of Bihar and or associated organizations including State health society, Bihar (SHSB) related to Aadhaar.

DOCUMENT CONTROL

Title	Information Security Policy	Signature & Date
Created by	System Analyst-cum- Data Officer, State Health Society, Bihar	
Reviewed by	Deputy Secretary / Departmental Information Security Officer, Health Dept., Govt. of Bihar	
Approved by	Secretary, Health Dept., Govt. of Bihar	

Document ID	Version No.	Classification	Owner
AADHAR_IS_01	**1.0**	**Restricted (Health Department)**	**CISO/Departmental Information Security Officer, Health Department, Govt of Bihar**

Document ID	Purpose	Review Frequency	Next Review
AADHAR_IS_01	**To define security controls for Aadhaar authentication usage as per UIDAI guidelines.**	**Annually**	**July 2026**

REVISION HISTORY

Document ID	Version	Effective From	Type of Change	Approved By
AADHAR_IS_01	1.0		First Version	Secretary, Health Dept., Govt. of Bihar

Terms & Definitions

S. No.	Terms	Definition
1	AAS	AADHAAR Authentication Server
2	API	Application Program Interface
3	AUA/ASA	Authentication User Agency/Authentication Service Agency
4	Asset	An asset is anything that has value to the organization. Assets can beclassified into the following 5 categories: 1. Paper assets: (Legal documentation, manuals, policies &procedures, organizational documents etc.) 2. Physical assets: (computer equipment, communications, utilityequipment, buildings etc.) 3. Software assets: (database information, applications, softwarecode, development tools, operational software etc.) 4. People assets: UIDAI human resources and stakeholders. 5. Service assets: (Logistics, building management systems,communications, utilities etc.)
5	CA	Certifying Authority
6	CIDR	Central Identities Data Repository
7	CN	Common Name
8	DPDP	Digital Personal Data Protection
9	Information/ Information Asset(IA)	Information that has value to the organization (UIDAI). Including but not limited to Citizen biometric and demographic information, personally identifiable information, employee information, organizationinformation such as CIDR details etc.
10	IT	Information Technology
11	KUA	Know your customer User Agency / e-KYC User Agency
12	MPoC	Management Point of Contact
13	NDA	Non-Disclosure Agreement
14	NTP	Network Time Protocol
15	OTP	One Time Password
16	PID	Personal Id entity Data
17	PPIUCD	Post-Partum Intra Uterine Contraceptive Device

18	PAIUCD	Post-Abortion Intra Uterine Contraceptive Device
19	RCA	Root Cause Analysis
20	SHS	Sate Health Society
21	SOP	Standard Operating Procedures
22	Sub-AUA	Sub Authentication User Agency
23	SPOC	Single Point of Contact
24	SSL	Secure Sockets Layer
25	STQC	Standard Testing and Quality Control
26	SBOM	Software Bill of Material
27	TPoC	Technical Point of Contact
28	VA	Vulnerability Assessment
29	VPN	Virtual Private Network

1. About the Policy

1.1 Policy Statement

Security of UIDAI Information Assets, handled by the Health Depart, Govt. of Bihar for providing services is of paramount importance of Health Department, Govt. of Bihar and its associated organizations, including State Health Society, Bihar and shall ensure the confidentiality, integrity, and availability of these at all times by deploying suitable controls commensurate with the asset value and in accordance with applicable rules.

1.2 Policy Scope

This Aadhaar Information Security Policy is applicable wherever UIDAI information is processed and/orstored by Health Department, Govt. of Bihar and its associated organizations, including State Health Society, Bihar. The policy may be amended from time to time as per regulations of UIDAI.

2 Information Security Domains and related Controls

2.1 Human Resources

1. Health Department, Govt. of Bihar shall appoint a Management Point of Contact (MPoC) and Technical Point of Contact (TPoC) for Aadhaar related activities and communication with UIDAI;
2. Health Department, Govt. of Bihar shall conduct a background check or sign an agreement/NDA with all personnel/agency handling Aadhaar related authentication data. UIDAI or agency appointed by UIDAI may validate this information.
3. Induction as well as periodic functional and information security trainings shall be conducted for Health Department, Govt. of Bihar and associated organizations on personal Aadhaar related authentication services. The training shall include all relevant security guidelines as per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhar Regulations, 2016.
4. All employees and 3rd party service providers accessing UIDAI Information Assets shall be made aware of UIDAI information security policy and controls.

2.2 Asset Management

1. All Assets used by the Health Department, Govt. of Bihar and associated organizations, including State Health Society, Bihar for the purpose of delivering services to beneficiaries of schemes mentioned in the scope above using Aadhaar authentication services shall be identified labelled and classified. Details of the Information Assets shall be recorded.

2. The assets (which are scheduled to be disposed) shall be disposed as per Health Department, Govt. of Bihar Information Security Policy;

3. Before sending any equipment out for repair, the equipment shall be sanitized to ensure that it does notcontain any UIDAI sensitive data;

4. Sub-AUA shall not transfer or make an unauthorized copy of any identity information from removable media to any personal device or other unauthorized electronic media / storage devices.

5. Sub-AUA shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets.

6. Authentication devices used to capture the Biometric of beneficiary shall be STQC (Standardization Testing and Quality Certification) certified as specified by UIDAI.

7. Endpoint Security:

   a. All endpoints and servers shall be hardened post-deployment using approved hardening checklists to minimize attack surfaces and eliminate default vulnerabilities

   b. Use of USB storage devices shall be restricted on all endpoints and prohibited on servers unless explicitly approved. Controls must be implemented to monitor or block unauthorized USB usage

   c. All IT assets must be protected by the latest, licensed antivirus/antimalware solutions with real-time protection enabled and regular updates configured through centralized monitoring tools

2.3 Access Control

1. Only authorized individuals shall be provided access to information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructureetc.) processing UIDAI information;

2. Health Department employees and third-party service providers with access to UIDAI information assets shall:

   a) Have least privilege access for information access and processing;

   b) The operator must be logged out after the session is finished.

   c) Implement an equipment locking mechanism for workstation, servers and/ or network device

3. All operators using assisted devices for Aadhaar authentication must authenticate using multi-factor authentication (MFA), combining at least two factors such as user ID/password, OTP/token, Aadhaar biometric authentication, or security questions.

4. The system must support and enforce MFA methods including, but not limited to, user credentials combined with OTP, biometric authentication (iris/fingerprint), security questions, or hardware tokens.

5. All assisted devices used in Aadhaar-based authentication (including PoS, enrollment kits, or tablets) must enforce MFA for operator access.

6. The authentication system must enforce MFA without exception and log all authentication

attempts for audit purposes. Lockout policies and alerts must be configured for repeated failed attempts.

7. The application should have auto log out feature i.e. after a certain time of inactivity (15 mins or as specified in the UIDAI Authentication Regulations document), the application should logout.

8. Access rights and privileges to information processing facilities for UIDAI information shall be revoked within 24 hours separation of respective personnel or as mentioned in the exit management policy of the organization Post deactivation, user IDs shall be deleted if not in use as per Exit formalities.

9. Access rights and privileges to information facilities processing UIDAI information shall be reviewed on a quarterly basis and the report shall be stored for audit purposes;

10. Common user IDs / group user IDs shall not be used. Exceptions/ risk acceptance shall be approved and documented where there is no alternative;

11. Procedures shall be put in place for secure storage and management of administrative passwords for criticalinformation systems. If done manually, then a fireproof safe or similar password vault must be used to maintain the access log register.

12. The users should not be provided with local admin access rights on their system. In the case of administrative access being provided, the users shall be prohibited from modifying the local security settings. Modifying the same shall result in disciplinary action.

13. Three successive login failures or as per the access control policy/password policy of the organization shouldresult in a user's account being locked; they should not be able to login until their account is unlocked andthe password reset in case of server logins. The user should contact the System Engineers/Administrators for getting the account unlocked. For applications, there should be an automatic lock out period of 30 minsin case of three consecutive login failures or as per the access control policy/password policy of the organization.

14. If the application is operator assisted, the operator shall first confirm his identity by authenticating himselfbefore authenticating the residents.

15. The access rules of firewalls shall be maintained only by users responsible for firewall administration.

16. This policy is aligned with UIDAI security guidelines for Aadhaar Authentication Agencies, mandating robust operator authentication mechanisms.

2.4 Password Policy

1. This password policy is developed in accordance with security best practices prescribed by UIDAI Aadhaar Authentication Guidelines.

2. The allocation of initial passwords shall be done in a secure manner and these passwords

shall bechanged at first login;

3. All User passwords (including administrator passwords) shall remain confidential and shall not beshared, posted, or otherwise divulged in any manner;

4. Keeping a paper record of passwords shall be avoided, unless this can be stored securely;

5. If the passwords are being stored in the database or any other form, they should be stored in encrypted form.

6. Passwords shall be changed whenever there is any indication of possible system or password compromise;

7. Strong passwords have the following characteristics:

   Contain at least three of the five following character classes:

   i. Lower case characters
   ii. Upper case characters
   iii. Numbers
   iv. Punctuation
   v. “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)

8. All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
9. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
10. The password should contain at least Eight characters.
11. All production system-level passwords must be part of the InfoSec administered global password management database.

2.5 Cryptography

1. The Personal Identity Data (PID) block comprising of the resident’s demographic~~/~~ /biometric data shall be encrypted as per the latest API documents specified by the UIDAI at the end point device used for authentication.

2. The PID shall be encrypted during transit and flow within the AUA ecosystem and while sharing this information with Aadhaar Service Agency (ASA); Logs of the authentication transactions shall be maintained but PID Information shall not be retained.

3. The encrypted PID block should not be stored unless in case of buffered authentication for not more than24 hours after which it should be deleted from the local systems;

4. The PID block shall be encrypted using AES-256 in CBC mode with a dynamically generated session key. This session key shall itself be encrypted using UIDAI's 2048-bit RSA public key as defined in the UIDAI Authentication API specification. The encrypted PID block shall also include a HMAC (SHA-256) to validate data integrity.

5. All biometric data (fingerprint/iris) must be encrypted at the time of capture using AES-256-

CBC. Biometric sensors must be STQC-certified and compliant with UIDAI biometric standards (L0/L1). No raw or decrypted biometric data shall be stored or transmitted.

6. Private keys used for decrypting session keys shall be securely stored in FIPS 140-2 Level 3 compliant HSMs. Key rotation and expiry shall be managed per UIDAI's key management guidelines.

7. In buffered authentication scenarios, encrypted PID data shall be retained only for a maximum of 24 hours and must be securely deleted thereafter. No part of the PID, including biometric or demographic data, shall be stored in plaintext or within log files.

2.6 Operations Security

1. Health Department, Govt. of Bihar shall complete the AADHAAR Sub AUA on-boarding process before the commencement of formal operations;

2. Standard Operating Procedure (SOP) shall be developed for all information systems and services related to UIDAI operations. The SOP shall include the necessary activities to be carried out for the operation andmaintenance of the system or service and the actions to be taken in the event of a failure;

3. Persons involved in operational/development/testing functions shall not be given additional responsibilities in system administration processes, audit log maintenance, security review of system or process and which may compromise data security requirements;

4. Where segregation of duties is not possible or practical, the process shall include compensating controls –such as monitoring of activities, maintenance and review of audit trails and management supervision;

5. The Test and Production facilities-environments must be physically and/or logically separated.

6. The Operating System as well as the network services used for communication shall be updated with the latest security patches.

7. A formal Patch Management Procedure shall be established for applying patches to the information systems. Patches should be updated at both application and server level;

8. Periodic VA (Vulnerable Assessment) exercise should be conducted for maintaining the security of the authentication applications, Network / Infrastructure Devices and Websites. Reports shall be generated and shared upon request with UIDAI.

9. Health Department, Govt. of Bihar employees shall not intentionally write, generate, compile copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any PID (Personal ID Entity Data) information;

10. All hosts that connect to the AADHAAR Authentication Service information shall be secured using endpoint security solutions. At the minimum, anti-virus-malware detection software shall be installed onsuch hosts;

11. Health Department, Govt. of Bihar / its System Integrator (SI) shall ensure that the event logs are to be recorded and stored to assist in future investigations and access control monitoring;

12. Regular monitoring of the audit logs shall take place for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorizedpersonnel only;

13. The authentication audit logs should contain, but not limited to, the following transactional details:

    a) Aadhaar Number against which authentication is sought;

    b) Specified parameters of authentication request submitted;

    c) Specified parameters received as authentication response;

    d) The record of disclosure of information to the Aadhaar number holder at the time of authentication

    e) Record of the consent of Aadhaar number holder for the resident

    f) Details of the authentication transaction such as API Name, AUA / KUA Code, Sub-AUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-identity information.

14. Network intrusion and prevention systems should be in place;

15. Logs shall not, in any event, retain the PID, biometric and OTP information;

16. The logs of authentication transactions shall be maintained by SHS, Health Department, Govt. of Bihar for a period of 2 years, during which an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified;

17. Upon expiry of the period of 2 years, the logs shall be archived for a period of 5 years or the number of years as required by the laws or regulations of Govt. of India, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by court or for any pending disputes;

18. All computer clocks shall be set to an agreed standard using a NTP (Network Time Protocol) server or must be managed centrally and procedure shall be made to check for and correct any significant variation;

19. The Sub AUA server host shall reside in a segregated network segment that is isolated from the rest of the networkof the SHS, Health Department, Govt. of Bihar, The AUA server host shall be

dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities;

20. Aadhar authentication application design and service flow

a. The Aadhaar authentication application consists of user-facing assisted devices running the AUA client, which interacts with the ASA gateway over a secure channel. The ASA then forwards the encrypted authentication request to UIDAI's CIDR for processing and returns the authentication response.
b. The Aadhaar authentication flow includes PID block creation, secure encryption, packet transmission via ASA, and secure response handling from UIDAI. No sensitive information (PID/biometric) is retained post authentication.
c. The application architecture includes the following components:

    1. Assisted Devices / Operator Terminals (Sub-AUA client)
    2. AUA Server (middleware application)
    3. ASA Gateway
    4. UIDAI CIDR (authentication backend)

All communication between these components is encrypted using **TLS 1.2 or above**. The application adheres to UIDAI's Authentication API specifications.

d. The authentication data flow proceeds as follows:

    i. The user enters their Aadhaar number or Virtual ID and provides biometric/OTP input on the client application.
    ii. The client generates the PID block and encrypts it using AES-256; the session key is encrypted with UIDAI's 2048-bit RSA public key.
    iii. A digitally signed authentication request packet is created and transmitted to the ASA.
    iv. ASA forwards the request to UIDAI CIDR for validation.
    v. The authentication response (Yes/No + code) is sent back via ASA and shown to the operator/user.
    vi. No PID, e-KYC, or biometric data is retained at any point.

e. The application includes the following security controls:

    i. Input validation at the client and server ends
    ii. Enforced use of UIDAI-certified encryption algorithms (AES-256, RSA-2048)
    iii. Secure key storage using HSMs or equivalent protected infrastructure
    iv. Role-Based Access Control (RBAC) for all application interfaces
    v. Secure API authentication and session management

f. Logs are maintained only for audit and dispute resolution purposes and include non-sensitive metadata such as masked Aadhaar/VID, timestamp, transaction ID, and error codes. No PID, biometric data, or e-KYC content is logged or stored in any application tier.
g. In case of failure or UIDAI unavailability, the system gracefully handles the error, logs the appropriate code, and ensures no retry of the same encrypted PID. Any buffered data is automatically deleted within 24 hours in compliance with UIDAI guidelines.

21. Secure Software Development Lifecycle

    a. All applications and systems developed or maintained in-house or by third-party vendors must follow a defined Secure Software Development Lifecycle (SSDLC) process that integrates security at each phase of development.

b. Security requirements, including data handling restrictions and encryption mandates (AES-256, RSA), must be captured at the start of the project.

c. Threat modeling must be conducted to identify risks to resident data and Aadhaar authentication workflows.

d. Developers must follow secure coding practices aligned with OWASP and must not use any deprecated or vulnerable libraries.

e. Security testing, including SAST and DAST, must be performed on all applications prior to production deployment.

f. Production deployment must be preceded by a security sign-off and configuration compliance verification.

g. Application components must be regularly updated, and any Aadhaar-related module must be reviewed post any UIDAI policy change.

h. Production deployment must be preceded by a security sign-off and configuration compliance verification.

i. Any third-party application integrated with Aadhaar authentication must comply with UIDAI SSDLC expectations and undergo independent security testing.

j. All personnel involved in application development shall undergo annual training on secure coding and Aadhaar-related data security

2.7 Communications security

1. All communication between Sub-AUA/Sub-KUA and their parent AUA/KUA must occur over secure, encrypted channels. VPNs, dedicated leased lines, or MPLS with TLS 1.2 (or above) encryption must be used. No Aadhaar-related traffic shall be transmitted over public or unsecured networks.

2. Authentication requests and responses must be transmitted using UIDAI-compliant secure protocols. Mutual authentication and IP whitelisting between endpoints shall be enforced to ensure integrity and confidentiality.

3. All Aadhaar authentication systems, including servers handling PID/authentication traffic, shall be deployed in a **dedicated, segmented network zone**. This zone must be isolated from general IT infrastructure using firewall rules, VLANs, or DMZ architecture.

4. Only authorized systems (e.g., AUA servers, ASA endpoints) shall be allowed to communicate with Aadhaar servers. Inbound and outbound traffic to this segment must be strictly controlled and logged.

5. Internet access on all Aadhaar-related systems (e.g., authentication servers, operator desktops, assisted devices) shall be **restricted to essential business-related websites only**. This shall be enforced using web filtering, proxy controls, and allowlisting mechanisms.

6. In case of a composite terminal device that comprises of a biometric reader without embedded software to affect the encryption of the personal identity data, communication between the biometric reader and the device performing the encryption shall be secured against all security threats / attacks

7. Terminal devices shall provide different logins for operators. These users shall be authenticated using someadditional authentication scheme such as passwords, AADHAAR authentication, etc.;

8. Each terminal shall have a unique terminal ID. This number must be transmitted with each transaction alongwith UIDAI assigned institution code for the AUA as specified by the latest UIDAI API documents

9. A Unique Transaction Number (unique for that terminal) shall be generated automatically by the terminalwhich should be incremented for each transaction processed;

10. The Sub AUA server shall be hosted behind a firewall. The firewall rules shall block incoming access requeststo the AUA server from all sources;

11. Special consideration should be given to wireless networks due to the poorly defined network perimeter. Appropriate **authentication**, **encryption**, and **user-level network access controls** should be implemented to secure access to the wireless network. All wireless communications, especially those involving sensitive data or Aadhaar authentication systems, must use **the latest stable version of Transport Layer Security (TLS), currently TLS 1.2 or above**, to ensure secure encryption during data transmission. Legacy protocols such as SSL, TLS 1.0, and TLS 1.1 shall be strictly disabled;

12. Use of web-based e-mail shall be restricted to official use and in accordance with the acceptable usage guidelines or as per organization policy;

13. UIDAI should be informed about the ASAs, the Sub AUA has entered into an agreement;

2.8 Information Security Incident Management

1. Health Department, Govt. of Bihar shall be responsible for reporting any security weaknesses, any incidents, possible misuse, or violation of any of the stipulated guidelines to UIDAI immediately.

2. Health Department, Govt. of Bihar shall ensure that the its employees & concerned Agencies / Vendors are aware about Aadhaar Authentication related incident reporting.

3. Root Cause Analysis (RCA) shall be performed for major Aadhaar related incidents identified in

its as well as its Agencies / Vendors ecosystem.

4. Any confidentiality breach/security breach of Aadhaar related information shall be reported to UIDAI within 24 hours.

5. From the effective date of sub-section (6) of section 8 of the DPDP (Digital Personal Data Protection) Act, report any personal data breach to the Data Protection Board and notify each affected individual within the time specified by the Act's rules.

6. Contact Details for Reporting and Escalation:

   Department Name: Health Department, Govt. of Bihar
   Chief Information Security Officer / Departmental Information Security Officer
   Email: health-bih@nic.in
   Phone: 0612-2215809
   Address: Vikash Bhawan, Bailey Road, Patna – 800015

2.9 Personal Data collection

1. Health Department, Govt. of Bihar and Associated Organizations, including State Health Society, Bihar shall collect the personal data including Aadhaar number/Virtual ID, directly from the Aadhaar number holder for conducting authentication with UIDAI at the time of providing the services;

2.10 Specific purpose for collection of Personal data

1. The Identity information including Aadhaar number / Virtual ID shall be collected for the purpose of authentication of Aadhaar number holder to provide scheme Benefits.

2. The identity information collected and processed shall only be used pursuant to applicable law and as permitted under the Aadhaar Act 2016 or its Amendment and Regulations.

3. The identity information shall not be used beyond the mentioned purpose without consent from the Aadhaar number holder and even with consent use of such information for other purposes should be under the permissible purposes in compliance to the Aadhaar Act 2016.

4. Process shall be implemented to ensure that Identity information is not used beyond the purposes mentioned in the notice/consent form provided to the Aadhaar number holder.

5. Notice / Disclosure of Information to Aadhaar number holder

6. Aadhaar number holder shall be provided relevant information prior to collection of identity information / personal data. These shall include:

   a) The purpose for which personal data / identity information is being collected;

   b) The information that shall be returned by UIDAI upon authentication;

   c) The information that the submission of Aadhaar number or the proof of Aadhaar is mandatory or voluntary for the specified purpose and if mandatory the legal provision mandating it;

d) The alternatives to submission of identity information (if applicable);

e) Details of Section 7 notification (if applicable) by the respective department under the Aadhaar Act, 2016, which makes submission of Aadhaar number as a mandatory or necessary condition to receive subsidy, benefit or services where the expenditure is incurred from the Consolidated Fund of India or Consolidated Fund of State. Alternate and viable means of identification for delivery of the subsidy, benefit or service may be provided if an Aadhaar number is not assigned to an individual;

f) The information that Virtual ID can be used in lieu of Aadhaar number at the time of Authentication;

7. Aadhaar number holder shall be notified of the authentication either through the e-mail or phone or SMS at the time of authentication and the Health Department shall maintain logs of the same;

2.11 Obtaining Consent

1. Upon notice / disclosure of information to the Aadhaar number holder, consent shall be taken in writing or in electronic form on the website or mobile application or other appropriate means and Health Department, Govt. of Bihar shall maintain logs of disclosure of information and Aadhaar number holder's consent.

2. Legal department shall be involved in vetting the method of taking consent and logging of the same, and formal approval shall be recorded from the legal department;

3. Consent for Aadhaar authentication shall be obtained in an accessible and informed manner for individuals with visual or hearing impairments. For visually impaired persons, consent shall be provided through screen readers, audio prompts, or verbal explanation by the operator. For hearing-impaired persons, consent shall be provided through clearly written formats or with sign language support if required. The method of obtaining consent shall be recorded without storing any sensitive personal data.

2.12 Personal Data Protection

1. Aadhaar authentication or Aadhaar e-KYC shall be used for the specific purposes declared to UIDAI and permitted by UIDAI. Such specific purposes shall be notified to the residents / customers / Individuals at the time of authentication through disclosure of information notice;

2. Health Department, Govt. of Bihar shall not use the Identity information including Aadhaar number or e-KYC for any other purposes than allowed under Aadhaar Act 2016 and it is associated Regulation and informed to the resident / customers / individuals at the time of Authentication.

3. For the purpose of e-KYC, the demographic details of the individual received from UIDAI as a response shall be used for identification of the individual for the specific purposes of providing the specific services for the duration of the services.

4. Data Protection related aspects under the Aadhaar Act, the regulation made thereunder and the standards and specifications issued by UIDAI and other regulatory authorities from time to time shall be adhered.

2.13 Sharing of Personal data

1. Identity information shall not be shared in contravention to the Aadhaar Act 2016, its Amendment, Regulations and other circulars released by UIDAI from time to time.

2. Biometric information collected shall not be transmitted over any network without creation of encrypted PID block as per Aadhaar Act and regulations;

2.14 Data Privacy on Aadhaar and Biometric details

1. The submission of Aadhaar details by beneficiary of schemes (As mentioned in scope above) is voluntary and Health Department, Govt. of Bihar and its associated organizations, including State Health Society, Bihar shall not insist on a beneficiary to produce their Aadhaar details for availing any of the services. In cases where Aadhaar number is offered voluntarily by the Beneficiaries to the Health Department, Govt. of Bihar, the Health Department and its associated organizations, including State Health Society, Bihar shall seek a declaration by the Beneficiaries towards the same.
2. For cases where e-KYC verification is required, the SHS, Health Department, Govt. of Bihar and its associated organizations, including State Health Society, Bihar shall get an explicit consent from the beneficiaries for download of resident demographic details from UIDAI mentioning the purpose for which the details are sought.
3. The consent shall be either in the form of an authorization letter or a provision to electronically record the consent in a software application.
4. The biometric details whenever captured by the Health Department, Govt. of Bihar and its associated organizations, including State Health Society, Bihar shall be used only for data exchange with UIDAI which validates the captured biometric data against the biometric data maintained in CIDR (Central Identities Data Repository) against the specific Aadhaar number.
5. Health Department, Govt. of Bihar and its associated organizations, including State Health Society, Bihar shall use STQC certified devices for demographic details received from UIDAI will be stored for future reference, the biometric details shall not be stored by the Health Department, Govt. of Bihar and its associated organizations, including State Health Society, Bihar in any manner and form.
    a. Assisted devices and applications used by Health Department, Govt. of Bihar and its associated organizations, including State Health Society, Bihar for Aadhaar authentication or e-KYC shall be strictly prohibited from storing Aadhaar numbers, e-KYC responses, or biometric data in any manner or form — either temporarily or permanently — in the device, application, or any associated storage (including cache, memory, or logs).

b. These devices and applications shall operate in a **stateless, pass-through** mode, transmitting authentication data directly to UIDAI without retention.

6. A system log wherever required shall be maintained to extract the details in case of disputes. The logs should capture Aadhaar Number, timestamp etc., but will not capture/store the PID (Personal Identity Data) associated with the transaction.

7. The data so captured will be sent to UIDAI as a straight through process. Health Department, Govt. of Bihar and its associated organizations, including State Health Society, Bihar shall not store the data captured (both biometric and personal information) in any manner and form.

   a. The Virtual ID (VID) or Aadhaar Number Capture Services (ANCS) token used during Aadhaar authentication shall be used **only for one-time, session-based transmission** to UIDAI and shall **not be stored** on any assisted device, application, or at the Sub-AUA/Sub-KUA server.

   b. Operators and systems are explicitly prohibited from caching, retaining, or reusing VID or ANCS tokens for any future transactions.

8. Access to full Aadhaar numbers shall be restricted based on the principle of least privilege. Where display is necessary, appropriate data masking techniques shall be employed such that **only the last four digits** are visible by default.

   a. Under no circumstances shall full Aadhaar numbers, biometric information, e-KYC details, or Virtual IDs be displayed on public interfaces, operator dashboards, receipts, or printouts.

   b. Display and disclosure of Aadhaar information shall be limited strictly to what is necessary for transaction validation and shall comply with Section 29 of the Aadhaar Act and UIDAI circulars on masking and data protection.

9. Identity information processed for Aadhaar authentication shall be protected against unauthorized access, display, or transmission. All third parties (including Sub-AUAs, Sub-KUAs, and business correspondents) shall be contractually bound to adhere to equivalent privacy and security standards.

10. Personally Identifiable Information (PII), including Aadhaar numbers, shall be classified as sensitive information and must not be disclosed or published in public domains (e.g., websites, portals, public reports). Controls shall be enforced to prevent accidental or deliberate exposure.

11. All personnel, including those of Sub-AUA / Sub-KUA and their affiliates, shall be explicitly prohibited from developing, introducing, or propagating any form of malicious code (e.g., viruses, worms, trojans, or logic bombs) that could compromise the confidentiality, integrity, or availability of Aadhaar-related systems or data.

12. Intentional actions that may impair system performance, restrict access, or result in unauthorized manipulation of Aadhaar data shall be treated as gross misconduct and be subject to disciplinary and legal action.

13. Preventive controls, including malware protection, system hardening, and integrity checks, must be implemented and monitored regularly to ensure system resilience against such threats.

3.Third party access and Outsourcing

3.1 Health Department, Govt. of Bihar, and its associated organizations, including State Health Society, Bihar shall ensure that third party access to information should be restricted andshould only be shared after signing Non-Disclosure-Agreement.

3.2 Wherever any activity is outsourced or awarded as service contract to any 3rd party / vendor,it shall be ensured that the contract specifies the information security requirements, and the same are complied with, in addition to the regular contractual details.

3.3 The following information security requirements should be documented as part of the contract:

i. General policy on information security.
ii. Procedures to protect organizational assets.
iii. Restrictions on copying / disclosure.
iv. Controls to ensure return of information/assets in their possession at the end of the contract.
v. The right to monitor and the right to terminate services in the event of a security incident or a security breach.
vi. Right to audit contractual responsibilities or to have the audits carried out by 3rd Parties.
vii. Arrangements for reporting, notification and investigation of security incidents and breaches.

3.4 Information security audit report of the vendor to be made available to Procuring entity on periodic basis or when required.

3.5 Detailed list of all components of the software (including open source) / solution in the form of Software Bill of Material (SBOM) shall be provided by the vendor. Vendor is also responsible for informing any identified vulnerabilities in the system to the organisation within reasonable time period.

3.6 Data collected and processed by the vendor should be protected appropriately (cannot be shared with any others without explicit consent / agreement) and made available to the procuring entity as and when required. External party personnel should comply with the information security policies, processesand procedures of the organisation.

3.7 Any external party found in violation to this policy shall be subjected to termination of contract and/ or will be handled as per applicable laws, rules & regulations.

4. Risk Assessment and security auditing requirements:

4.1 In case of any Risk, Health Department, Govt. of Bihar, and its associated organizations, including State Health Society, Bihar must hold meetings with all stakeholders and heads of the department to chalk out the requirements for security audits such as the following:

i. Scope of the audit
ii. Risk based asset classification
iii. Audit benchmarks, standards and compliance requirements
iv. Remediation plan on audit findings
v. Audit report format along with requirements of evidence and artifacts
vi. Follow-up audits
vii. Examine the effectiveness of the existing policy, standards, guidelines and procedures

4.2 Periodicity and nature of audits

i. Internal information security audit of Applications to be performed at least once in a year.

ii. 3rd Party Security audits must be conducted periodically at least once a year to ensure compliance with security policy, guidelines, and procedures, and to determine the minimum set of controls required to address Health Departments security.

iii. Security audit should be performed prior to and after implementation or installation or major enhancements in the Health Department, Govt. of Bihar, and its associated organizations, including State Health Society, Bihar.

iv. Follow-up audits should be conducted to ensure compliance and closure of vulnerabilities

5. Change Management

i. All changes to UIDAI Information Processing facilities/ Infrastructure/ processes shall be documented.

ii. Only those changes related to Aadhaar which are approved by UIDAI for execution shall be implemented.

iii. Change log/ register shall be maintained for all changes performed.