सत्यमेव जयते national health agency

Pradhan Mantri Jan Arogya Yojana
Ayushman Bharat

National Health Agency

Fundamentals on Security & Privacy

August 2018

Version 1.0

NATIONAL HEALTH AGENCY, ROOM NO. 343-A, NIRMAN BHAWAN, NEW DELHI

Introduction

Security is the responsibility of us all. This training manual introduces basic Information security and privacy requirements at State and District level.

Target Audience

- Arogya Mitra
- Enrolment Agencies
- Hospital Staffs
- Empaneled Doctors
- Claim Processors
- Insurers
- Technical Support staff
- Anyone who wants to know about the best practices

Things to "DO" while collecting Beneficiaries Personal Data

Taking "Consent" from Beneficiaries is mandatory while collecting Aadhaar Data or Health Data

Obtain Beneficiaries consent electronically prior to collecting their information. Both BIS & TMS application has an option to collect consent prior to seeking beneficiaries' information.

Aarogya Mitra or any individual who are collecting KYC/health information of a beneficiary shall ensure consent is obtained in the applications.

Inform the beneficiaries clearly about the data being collected, and its usage.

Ensure Consent form is also provided in local language and beneficiary has complete understanding about the usage and data being collected from them.

Is there any exception to above?

Child Consent: Parent or legal guardian can give consent on behalf a child below the age of 18 years, provided a valid proof of relationship (PoR), proof of identity (PoI) and proof of age of the child is submitted.

Beneficiaries who are seriously ill or mentally incapacitated: Any adult member of the family can give consent, based on proof of relationship (PoR) along with proof of medical condition of the individual

Ensure only authorized beneficiary is handed over with ABPMJAY ID Card

Perform complete identity check prior to identifying anyone as beneficiary of the Ayushman Bharat Scheme.

Do seek Supervisory comments in case of any confusion

Respect Privacy of others – Limit Disclosure

Disclose information only to the owner of the information.

Example, if Rama is beneficiary, then information of Rama should only be handed over to Rama post verifying his Identity

Respect Individual Rights – Provide Choice

Do not force Beneficiary to share his consent

Provide them choice to share their data with us under their consent

Inform that they can revoke consent anytime they want with a written notice

Sign Non-Disclosure Agreement

Ensure you have signed Non-Disclosure Agreement (NDA) with National Health Agency (NHA) prior to starting your journey as Aarogya Mitra

How to Handle Beneficiaries Information?

Handle Beneficiaries Information Confidentially

Discuss beneficiaries’ sensitive data (Ex: health data) in private.

If possible, point out on paper or on-screen nonverbally when discussing beneficiary’s sensitive data (ex: health data)

Don’t respond to emails or phone calls requesting confidential company information—including employee information, financial results or company secrets.

Handle Beneficiaries Information Securely

Shred all hard copies containing sensitive personal data when the copies are no longer needed.

Do not leave sensitive personal data (files, records, Rolodex, reports) exposed, open, or unattended in public areas, conference rooms, mailboxes, wall trays, etc.

Store all sensitive personal data securely in locked file cabinets, desk drawers, offices, or suites when you are not in your work area.

Delete all soft copy files containing sensitive personal data from your computer and from the server when the information is no longer needed within the record retention requirements.

Destroy all disks, CDs, etc., that contained sensitive personal data before disposing them.

Do not reuse disks, CDs that contained sensitive personal data without sanitizing them first.

Contact “Tech Support Team” before transporting or transferring equipment for proper procedures to move equipment and to sanitize hard drives and other media.

Return the sensitive personal data to the sender, if this requirement is stipulated in any contractual agreements.

Email

Do not include any Sensitive data (ex: health data) in Subject-line or in Body of email.

Transmit Sensitive data only in a password-protected attachment (MS Word and MS Excel provide password protection).

Include a confidentiality statement on emails that contain any Sensitive data in email attachments.

Do not send attachment passwords in the same email as the attachment.

Request that email recipients call to discuss specific participant data.

Do not store emails or email attachments with Sensitive data on your Desktop/Laptop.

How to Protect my Account & Password?

Never share your user ID & password with anyone.

Do not write your password anywhere in the computer/laptop/ any paper/diary.

Don't use "Easy to guess" passwords,

Do not use user name as password.

Do not reuse last 5 passwords

Your account will be locked post 3 successive login failures. Contact the tech support for getting the account unlocked

Change your password on regular basis (at least once in 90days).

Example of "Easy to Guess" Password:

"Password"   "CAT"   "India"   "12345" "Mobile number"   "Birth date"

How to act in case of any Security Incidents?

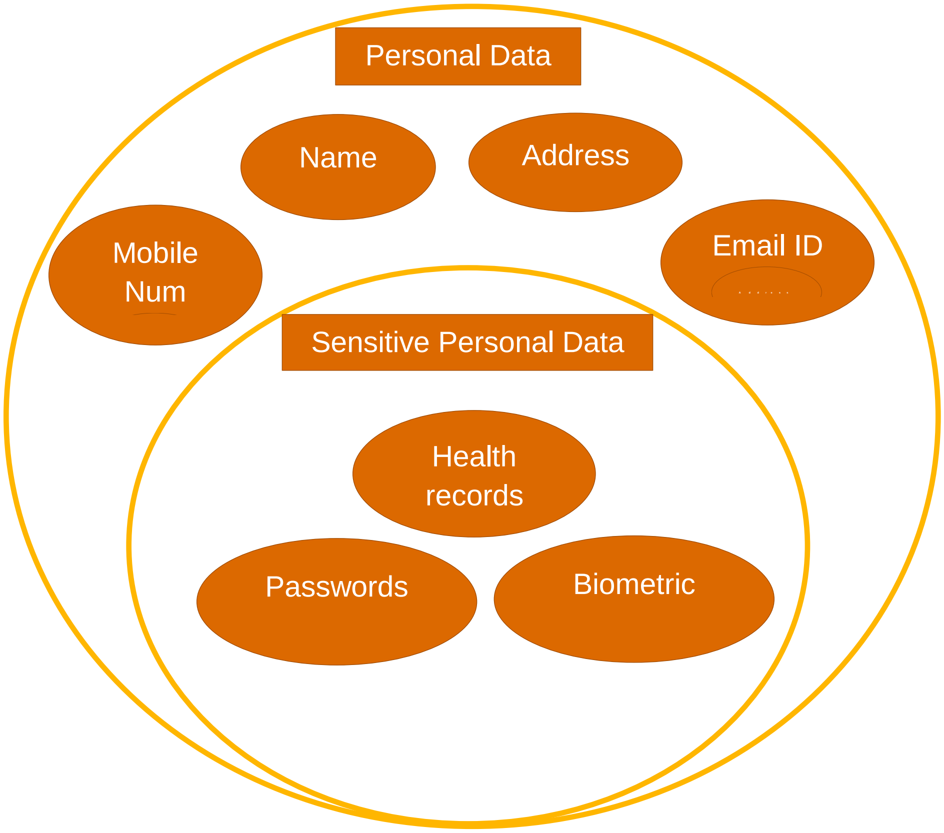
In case you find any unauthorized/ suspicious activities occurring, report it immediately to the hospital authority to bring it into the notice of SHA for necessary action.

Example:

The equipment used for authentication is lost or theft.

You notice any unusual activity on your system or the applications

What is Personal & Sensitive Personal Data?



How to protect our Computer? (For Tech Support Team)

1. **Password Protection-** Adequate security controls such as password protection (minimum 8 characters including at least one uppercase letter, lowercase letter, number, alphanumeric character) should be implemented on the system at the enrolment center.
2. Restrict Wi-Fi password within the office premise only. Change (e.g., in every three months) the user password to access the Wi-Fi periodically
3. **Anti-virus software-** Anti-virus / malware detection software should be installed to protect the information against malwares/viruses**.**
4. **Only commercial software's to be used-** Only licensed version of Operating System should be installed on the systems, and should be configured to automatically download the latest security patches released by the vendor.
5. **Unauthorized software's should not be used** – Only authorized and licensed software's should be installed and used on the enrolment systems.
6. **USB devices to be used**- Only sanitized (virus free) USB devices should be used to transfer enrolment packets for the purpose of back up and upload to CIDR.
7. **A clear desk and clear screen policy** for beneficiaries' information processing facilities shall be adopted to reduce risks of unauthorized access, loss and damage to information. Ensure screen saver or related technological controls to be implemented to lock the screen of the information systems when unattended beyond a specified duration. Turn off the computer, or log out of the network when not at your desk.
8. Position screens so they are not visible to others. Do not leave laptop or work-related participant sensitive personal data visible or unsecured in a car, home office, or in any public areas.
9. Ensure that all sensitive personal data used outside work premises is protected using appropriate measures such as locked desks, file cabinets.
10. Never remove original copies of sensitive personal data from the agency without your supervisor's approval for specific purposes.
11. Do not Store files that contain Aadhaar data/health data/any sensitive data of beneficiaries on your workstation hard drive.
12. Do not collect Copy of Aadhaar unless explicitly asked for.