national health agency
सत्यमेव जयते
arogya Samvad
Pradhan Mantri Jan Arogya Yojana
Ayushman Bharat
PM-JAY
"AROGYA SAMVAD" Newsletter for AYUSHMAN BHARAT - Pradhan Mantri Jan Arogya Yojana ISSUE 2, December 2018

Sec rity is incomplete without "U"

Safeguarding the nation's critical IT infrastructure is everyone's responsibility

The entire backbone of Ayushman Bharat is based on a critical infrastructure which is supporting the mega health insurance scheme. A disruption to these services, most of which are operated via internet, can result in catastrophic consequences.

Threats to information security come in all shapes and sizes

Using guessable passwords

Easy to guess password/ writing password may give access to the adversary to perform action like stealing sensitive information of beneficiaries as a proxy to the actual user. Such type of attacks are irremediable and generally backfires at the account owner.

Malware Infected Machines

The SHA's have the ability to upload data files on NHA's server, which if done using infected machine poses serious threat.

Clicking on luring advertisements

SHA's employees having access ID for NHA's portal and servers may fall in trap of phishing campaign which may lead to unauthorized people gain access of these portals containing highly sensitive information of beneficiaries.

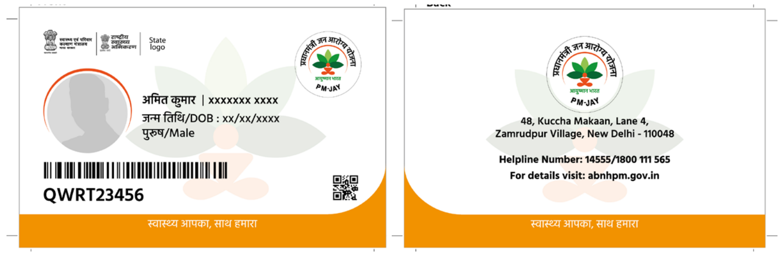
Outdated antivirus

Not updating antivirus softwares regularly may make systems vulnerable and allow malicious files to enter the SHA system and thus in NHA network. These malicious files may crash the entire IT infrastructure of the agency.

Unknown E-mail/ Attachments

Opening attachments from unknown sources may lead to the entry of viruses, Trojan, malware in the network which will dwell in the network and send information to hackers outside the network.

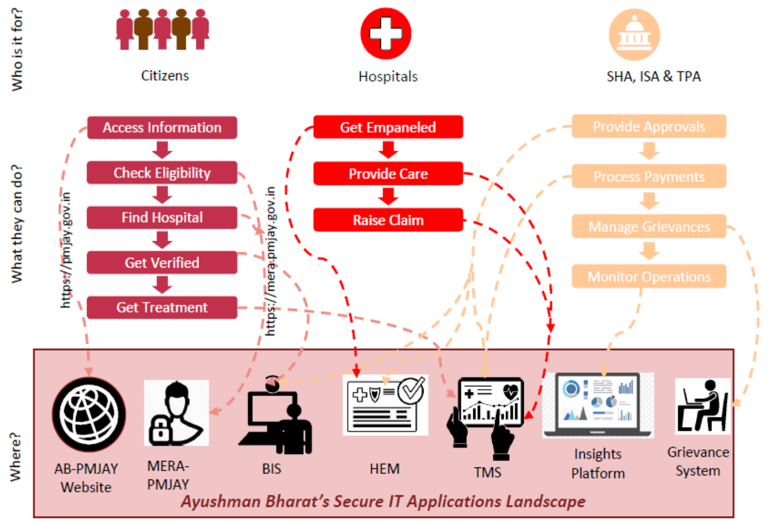
Mission: Patching Humans


स्वास्थ्य एवं परिवार कल्याण मंत्रालय
राष्ट्रीय स्वास्थ्य अभिकरण
State logo
प्रधानमंत्री जन आरोग्य योजना
आयुष्मान भारत
PM-JAY
अमित कुमार | xxxxxxx xxxx
जन्म तिथि/DOB : xx/xx/xxxx
पुरुष/Male
QWRT23456
स्वास्थ्य आपका, साथ हमारा
48, Kuccha Makaan, Lane 4,
Zamrudpur Village, New Delhi - 110048
Helpline Number: 14555/1800 111 565
For details visit: abnhpm.gov.in
स्वास्थ्य आपका, साथ हमारा

A sample beneficiary e-card

No amount of technical controls can keep an organization 100% safe unless its people are aware of the information security threats and are alert at all times. Cyber attackers understand that the easiest intrusion vector is 'You'. Therefore, it is imperative to be cyber-aware. Here are some easy tips that everyone must practice to help protect the critical IT infrastructure:

Ayushman Bharat's robust IT backbone



Ayushman Bharat's Secure IT Applications Landscape

IT Joumey Since PM-JAY Launch

We have already made following major enhancements to our IT Platform:

- National Portability
- Common Service Centres have been enables to verify AB-PMJAY beneficiaries
- BIS State Approvers of all States will now be able to view/approve/recommend/reject records from a cluster list of districts/sub-districts
- Auto-Approval of Pre-Auth after 6 hours
- Optimized workflow for faster Pre-Auth initiation and discharge
- Two level authentication for login in HEM
- Feature to facilitate workflow changes from front end

What's Coming Next?

The following new features are being worked on and shall be made available in upcoming releases:

- Android Mobile App for TMS
- Bank Integration for direct payment to hospital from SHA
- Multiple pre-authorizations would be allowed for surgical cases
- Partial Payment for Special Cases
- Information update feature
- Integration of verification ID's
- Upgrade Specialities for empanelled hospitals
- Live Integration of HEM database with TMS
- Warehouse Integration with brownfield states
- Fraud Management Systems

When in doubt, throw it out

- Links in emails, tweets, posts and online advertising are common ways cybercriminals try to compromise your information. If it looks suspicious, its best to delete it.

- Email phishing is a form of social engineering where malicious emails are designed to deceive recipients into providing sensitive information, or clicking links or file attachments that install malware (e.g. viruses, spyware).

- Phishing or planting infected USB drives are a few of the common ways that exploit sensitive data.

Safer for me, more secure for all

- Using internet safely – What you do online affects everyone. Secure online habits reduce the opportunities for attackers to install malware or steal personal information of beneficiaries enrolled.

- Avoiding malicious sites, never ignore warning messages from your browser, never ignore 'Website security certificate' error.