



# Digitization in Healthcare

February 2023

Volume-7

**Copyright**

This edition of Information Technology made Handy for Doctors, Volume 7, February 2023 is published in joint association by – TIMSCDR and Association of Medical Consultants – AMC

ISBN 978-81-949693-0-3

February 2023, Volume 7

## **Editors**

**Dr. Vinita Gaikwad**

Director

Thakur Institute of Mgmt. Studies,  
Career Development & Research

**Dr. Mukesh Gupta**

Media & Communication Cell, AMC,  
Founder Director - LeNest

## **Contributors**

**Ms. Sonu Gupta**

**Ms. Rashmi Vipat**

**Ms. Aprajita Singh**

**Mr. Shirshendu Maitra**

**Ms. Rupali Jadhav**

**Mr. Brijesh Pandey**

**Ms. Kinjal Doshi**

**Ms. Monisa Rodrigues**

**Ms. Anamika Dhawan**

**Ms. Shweta Waghmare**

**Ms. Rohini Bagul**

**Ms. Thara C**

**Dr. Padma Mishra**

**Dr. Pinky Gerela**

**Ms. Alifiya Shaikh**



# Forward



**Dr. Nilima Vaidya  
Bhamare**

President – AMC

It has been a privilege for me personally and for AMC to associate with TIMSCDR since last seven years through this flagship event, International Conference – ICAIM .

This year ICAIM 2023 titled “Leveraging Information Technology for Sustainability in Agriculture and Healthcare - Carbon Neutrality” comes with yet another matter of public relevance i.e., Global Warming. Every sector is directly or indirectly contributing towards Global Warming. We are now required to take cognisance of the situation and move towards Carbon Neutrality.

ICAIM 2023 is a special platform for Healthcare professionals as every year the Conference conducts a training for updating the Doctors of Information Technology tools and how they can be used in their daily practice to offer better Healthcare to the patients.

Doctors workshop – “Digitization of Healthcare” bring forth the necessity of understating and to some extent using tools like Blockchain, Cyber Security, ChatGPT and converting a website into a mobile App. It also has instore sessions on ABHA Registration to be in line with our governments goal of ADBM.

I am definite that like the past several ICAIM’s – ICAIM 2023 is a sure shot success. I wish all the participant All the very Best. Congratulations to TIMSCDR and AMC for the successful accomplishment of ICAIM 2023.



# Preface



**Dr. Mukesh Gupta**  
Founder Director – Le'Nest,  
Past President – AMC



**Dr. Vinita Gaikwad**  
Director  
Thakur Institute of Mgmt. Studies,  
Career Dev. & Research

In the current Digital Era we cannot afford to remain novice to the various technical developments, specifically those in the Healthcare sector.

Though Digitization of Healthcare is picking up pace in India, it is far well established in the western countries. The Government of India has begun the work of Digitization in Healthcare through Ayushman Bharat Digital Mission (ABDM), which basically focuses on an integrated digital healthcare infrastructure. This infrastructure is rather intense, specifically for a developing country like India with a large population. The smallest element of this infrastructure is the EHR.

At a higher level, digitization is sharing of Health data of patients across setups like Government and Private Healthcare facilities. This would require ensuring that data travels seamlessly and securely across various network channels and platforms. Having the right infrastructure to perform this is of utmost significance.

The recent introduction of ABHA - Ayushman Bharat Health Account, which facilitates sharing and accessing Healthcare records under a unique identity indicates that all Healthcare professionals need to incorporate digitization at their respective Healthcare facilities.

Further, it is just not enough that we create the required infrastructure, but we also need to align to the changing digital trends. We need to be aware about the dangers of digital footprints specially in the Healthcare sector as majority of the data handled belongs to patients, demanding privacy.

ICAIM 2023 - Digitization of Healthcare is yet another happening event which opens up thought provoking deliberations amongst Healthcare and IT professionals on current topics of interest.

The “Digitization in Healthcare” workshop introduces the Doctors to several Technical aspects which are of current relevance when digitizing Healthcare.

Digitization is necessary. However, it needs to be implemented carefully and managed continuously and cautiously.



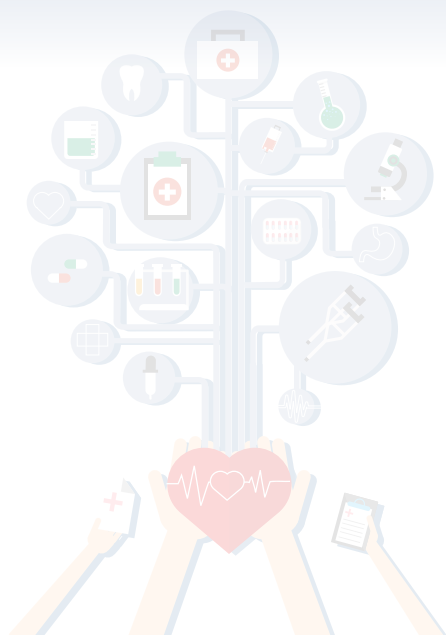


# Contents

<b>1. Basics of Blockchain and its Role in Healthcare - EHR .....</b>	<b>1</b>
➤ What is Blockchain? .....	1
➤ Usage of Blockchain .....	2
➤ Future of Blockchain Technology .....	2
➤ Blockchain based Cryptocurrency Transactions using MetaMask .....	2
• Introduction of MetaMask .....	2
• Setup A Metamask Ethereum Wallet .....	3
• Sending sample Ethereum from one account to another .....	5
• Pros & Cons of MetaMask .....	8
<b>2. Creation of ABHA Registration Number .....</b>	<b>9</b>
➤ What is ABHA? .....	9
➤ What does it provide? .....	10
➤ ABHA Registration .....	11
• Guide to create ABHA Number .....	11
• Guide to Link Health Locker with ABHA Number .....	13
• Guide of ABHA Healthcare Professional Registration .....	15
<b>3. UHI .....</b>	<b>17</b>
➤ What is UHI? .....	17
➤ UHI Services .....	18
➤ Benefits of UHI .....	18
➤ Stakeholders .....	18
• Citizen : Health ID .....	18
• Healthcare Services : Healthcare Facility Register .....	18
• Technology Service Providers .....	19
➤ UHI Sandbox .....	19
• What is UHI Sandbox .....	19
• Building UHI EUA App .....	19
<b>4. DigiLocker .....</b>	<b>21</b>
➤ ABHA Card Generation .....	21

5. Cybersecurity in Healthcare : The Foundation for Digital Transformation .....	23
➤ What is Cybersecurity in Healthcare? .....	23
• Healthcare Stakeholder .....	25
• Why Healthcare is a Prime Target for Cyber Criminals...? .....	26
➤ Biggest Cyber Threats in Healthcare .....	27
• Phishing .....	27
• How to Prevent Healthcare Phishing attacks? .....	28
• Ransomware and Other Malware .....	29
• How to detect and prevent Ransomware .....	30
• Healthcare Data Breaches .....	30
• DDos Attacks .....	33
• Hot Attack against Conferencing Software .....	34
➤ Cybersecurity in Healthcare Best Guidelines .....	35
• Risk Assessments .....	35
• Security Controls .....	36
➤ How to secure the system? What to do and what not to do.....	36
➤ Cybersecurity in Healthcare Laws and Regulations .....	44
6. Converting Website to Mobile Application .....	47
➤ Importance of Mobile Apps.....	47
➤ How Mobile Apps can improve your business?.....	49
➤ Convert your Website to Mobile App .....	51
➤ Step by Step Guide.....	51
7. Content Marketing – ChatGPT.....	57
➤ Open AI- ChatGPT .....	57
➤ Steps to use ChatGPT .....	58
➤ Advantages of ChatGPT.....	59
➤ Disadvantages of ChatGPT .....	60

# 1



## Basics of Blockchain and Its Role in Healthcare - EHR

### ➤ What is Block chain?

Block chain is decentralized electronic ledger that involves a peer-to-peer network. This peer-to-peer (P2P) network will digitally connect all the stakeholders in the value chain to maintain the accuracy of data.



➤ **Usage of block chain:**

Block chain uses in various sectors like agriculture, finance, and healthcare & in supply chain industry too

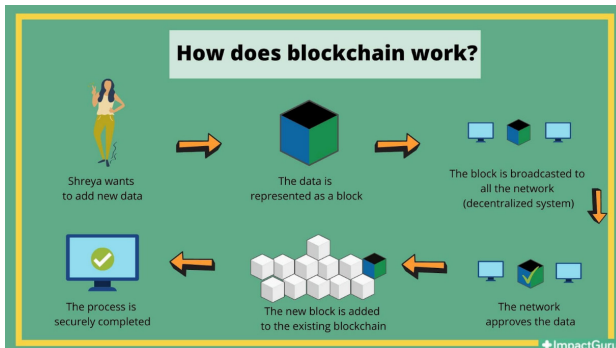
Block chain uses block technology to securely store health records and maintain a single version of the truth. The different organizations such as doctors, hospitals, laboratories, pharmacists & health insurance can request permission to access a patient’s record to serve there purposes and record transactions on the distributed ledger.



➤ **Future of block chain technology:**

Block chain technology has a very impactful effect on the healthcare industry when it comes to transparency, credibility, security, accessibility, effective cost, etc. Due to these advantageous factors, many considerable organizations are shifting from Centralized system to Decentralized system.

The chain would function as a shared ledger and would be controlled by a system of smart contracts.



➤ **Blockchain based Cryptocurrency Transactions using MetaMask**

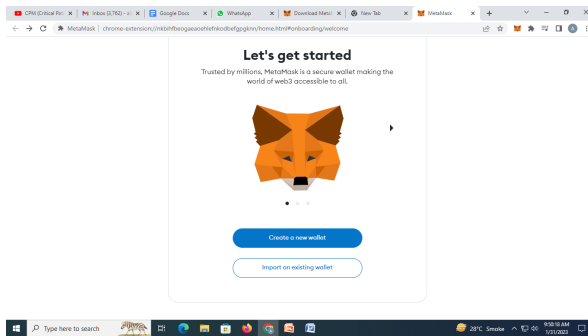
● **Introduction of Metamask:**

The meta mask was Launched by Aaron Davis in 2016 and is headquartered in San Francisco, MetaMask is a decentralized, non-custodial Ethereum-based wallet

that allows users to store, buy, send, convert, and swap crypto tokens. The wallet is available as a mobile app and browser extension on Google Chrome, Firefox, Opera, and Brave.



● Setup a Metamask Ethereum Wallet



Step 1: Install MetaMask & Add MetaMask extension to the Browser, Now here click on “Create a new wallet”

**Help us improve MetaMask**

MetaMask would like to gather usage data to better understand how our users interact with MetaMask. This data will be used to provide the service, which includes improving the service based on your use.

MetaMask will...

- ✓ Always allow you to opt-out via Settings
- ✓ Send anonymized click and pageview events
- ✗ Never collect information we don't need to provide the service (such as keys, addresses, transaction hashes, or balances)
- ✗ Never collect your full IP address\*
- ✗ Never sell data. Ever!

This data is aggregated and is therefore anonymous for the purposes of General Data Protection Regulation (EU) 2016/679.

\* When you use Infura as your default RPC provider in MetaMask, Infura will collect your IP address and your Ethereum wallet address when you send a transaction. We don't store this information in a way that allows our systems to associate those two pieces of data. For more information on how MetaMask and Infura interact from a data collection perspective, see our update here. For more information on our privacy practices in general, see our Privacy Policy here.

**Help us improve MetaMask**

MetaMask would like to gather usage data to better understand how our users interact with MetaMask. This data will be used to provide the service, which includes improving the service based on your use.

MetaMask will...

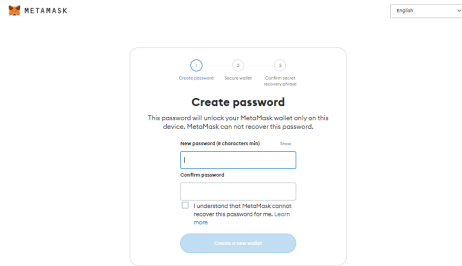
- ✓ Always allow you to opt-out via Settings
- ✓ Send anonymized click and pageview events
- ✗ Never collect information we don't need to provide the service (such as keys, addresses, transaction hashes, or balances)
- ✗ Never collect your full IP address\*
- ✗ Never sell data. Ever!

This data is aggregated and is therefore anonymous for the purposes of General Data Protection Regulation (EU) 2016/679.

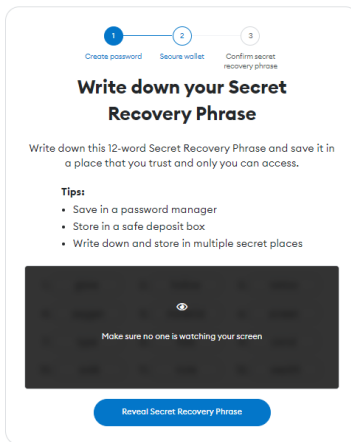
\* When you use Infura as your default RPC provider in MetaMask, Infura will collect your IP address and your Ethereum wallet address when you send a transaction. We don't store this information in a way that allows our systems to associate those two pieces of data. For more information on how MetaMask and Infura interact from a data collection perspective, see our update here. For more information on our privacy practices in general, see our Privacy Policy here.

Step 2: In next window click on “I agree” button

### Step 3: System will ask to create your own password



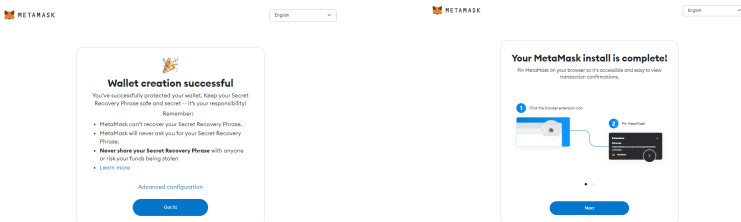
### Step 4: After creating the password MetaMask will show up 12 words recovery key (Seed).



- MetaMask will show up 12 words recovery key (Seed).

Step 5: store that 12 words in somewhere like notepad or excel, later we have to type that phrases in sequence so if you will forget the password these 12 words are the only way to restore MetaMask accounts.

After completing this task you will be able to create self-wallet successfully



## GAS IN ETHEREUM

The transaction fee is calculated in Gas, and paid for in Ether.

The gas is the "fuel" of the Ethereum network, which is used to:

- Conduct transactions
- Execute smart contracts
- Launch Dapps.

## WHAT IS ETHER?

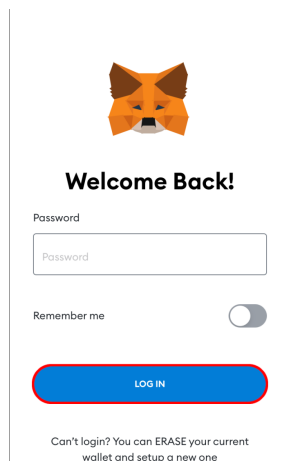
- Ether (ETH): is the Ethereum network's native cryptocurrency, the second-largest by market cap on the crypto market.
  - Gas indicates the fee for a particular action or transaction.
  - Gas Limit: is the maximum amount of Gas that a user is willing to pay for performing this action or confirming a transaction.
  - Gas Price: is the amount that the user is willing to spend on each unit of Gas.
- **Sending sample ethereum from one account to another**

Using metamask to transfer funds or ETH to another account is very simple

You just need to install the Metamask in your Desktop or mobile device

So here we will see how we can do the transactions between the account

Step 1: Open the metamask app & log in



Welcome Back!

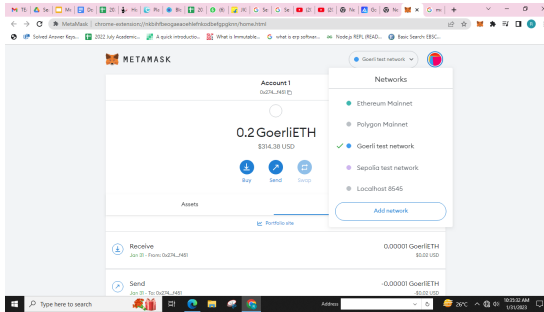
Password

Remember me

LOG IN

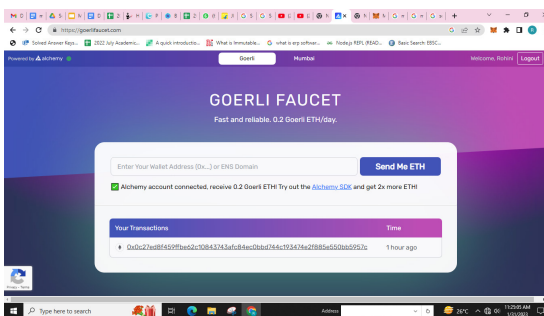
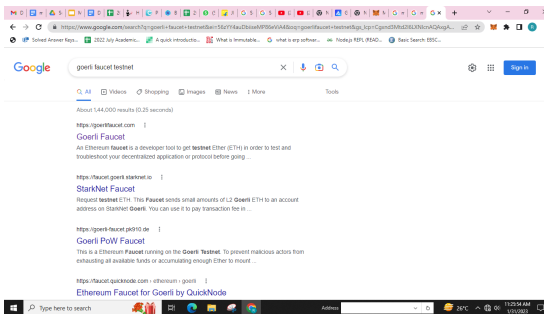
Can't login? You can ERASE your current wallet and setup a new one

Step 2: Open the test network to transfer dummy ETH



Step 3: Select any test network for eg. Goerli test Network

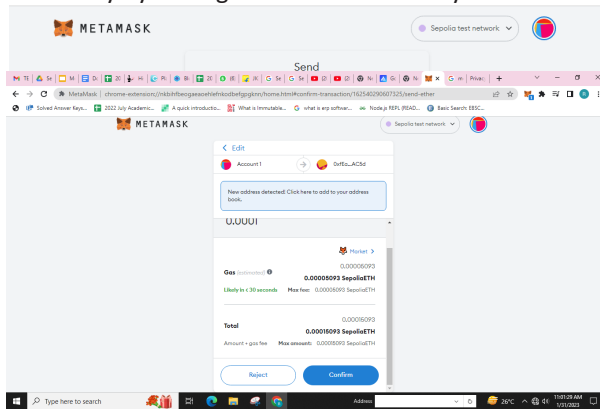
Step 4: When we open the bank account we have to deposit some amount to do further transactions so same in metamask we need some ETH to deposit in our account so how we can get sample eth? For that we have solution, there is websites like faucet which will give you the fake or sample ETH which we can use for testing purpose only. Simply type on Google with name of test network for eg. "Goerli Faucet". Now, click on the first option



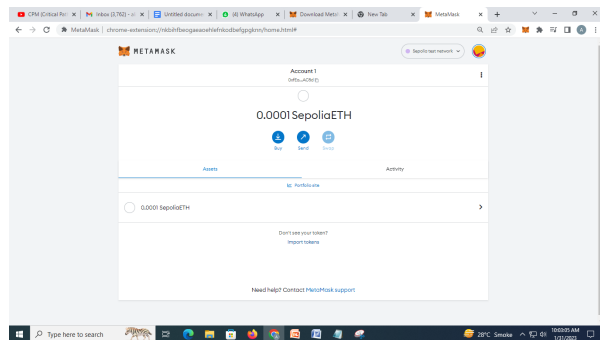
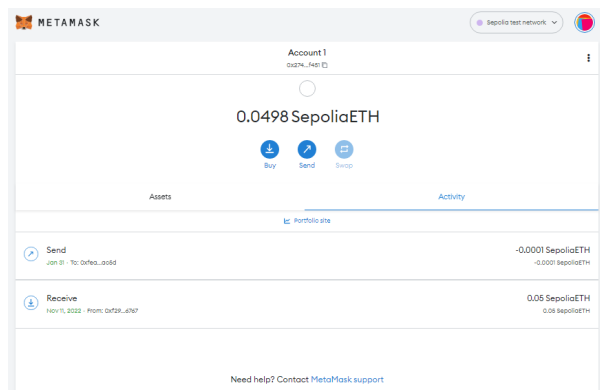
Step 5: Here paste the ETH account and click on the send me ETH so in your metamask account will get 0.2ETH



Step 6: After successfully adding Fake ETH in our metamask account we can send to another account easily by adding account address only



Step 7: So after successfully transferring ETH from one account to another it will show that some debited ETH from your account and credited ETH in another account.



So, this is how we done the transaction from one account to another using metamask

## ● Pros & Cons of MetaMask

Usually each software has their own advantages and limitations. Like we can see in metamask also we have following pros and cons.

Pros:

- Saving Cryptocurrency ( Secure Wallet )
- Trading
- Purchasing NFTs by minting them
- Used for playing games that require NFTs or Cryptocurrency

Cons:

- Saving Cryptocurrency ( Secure Wallet )
- Trading
- Purchasing NFTs by minting them
- Used for playing games that require NFTs or Cryptocurrency

# 2



## Creation of ABHA Registration Number

### ➤ What is ABHA?

Participants in India's digital healthcare ecosystem receive a unique Identity via their Ayushman Bharat Health Account. A 14-digit ABHA number is given to each account, which will be used to identify customers.

Your ability to exchange and access your health information online is made possible by your ABHA (Ayushman Bharat Health Account) Address, a distinctive identifier (self-declared username). Your ABHA address could be in the format of "yourname@consent manager"..For instance, xyz@abdm is a ABHA address with ABDM Consent Manager that will facilitate health data exchange for you with appropriate consent on the ABDM network.

To quickly register for an ABHA address and guarantee that the health data made for one are shared exclusively with healthcare professionals, use your ABHA number. It is advised that you establish an ABDM ABHA address and link it to your ABHA number in order to permit the sharing of health data..

Participation is free, and individuals have the option to voluntarily establish an ABHA number. Additionally, one may request the permanent deletion or short-term deactivation of their ABHA number at any moment.

## **What is NDHM? What is ABDM?**

National Digital Health Mission (NDHM) is pilot project which was launched by Honorable Prime Minister on 15th August 2020 in the six union territories of Ladakh, Chandigarh, Dadra and Nagar Haveli and Daman and Diu, Puducherry, Lakshadweep and Andaman and Nicobar Islands. The nationwide rollout of this pilot project was announced by Hon'ble Prime Minister Shri. Narendra Modi on 27th September 2021 with the name "Ayushman Bharat Digital Mission" (ABDM).

## **What is HPR?**

The HealthCare Professionals Registry is a comprehensive database of licenced and vetted professionals providing both contemporary and conventional medical healthcare across India

## **What is PHR?**

PA self-declared username known as PHR (Personal Health Records) Address is needed to access a Health Information Exchange & Consent Manager (HIE-CM). To facilitate data exchange, each ABHA number must be linked to a consent manager

## **ABHA App**

The Ayushman Bharat Health Account (ABHA) smartphone application of the Indian government was released by the National Health Authority (NHA) as part of its flagship programme, the Ayushman Bharat Digital Mission (ABDM) (GoI). Through the ABDM network of various healthcare institutions and providers, the ABHA Mobile application offers users a longitudinal view of their health records with the possibility to link and share them after user approval.

## ➤ **What does ABHA provide?**

It provides following:

### **1. Health identity for every citizen**

One can link their own health record

### **2. Healthcare Professionals registry**

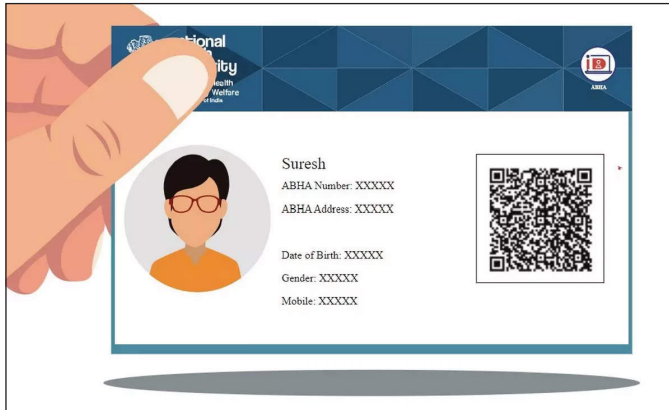
A central location for all healthcare professionals.

### **3. Healthcare Facilities Registry**

Makes sure physicians and hospitals can conduct business easily

## **Salient Features:**

1. C1. Using a variety of data, information, and infrastructure services, create an online platform that is seamless.
2. Enable the interchange of people's long-term health records with their permission.
3. Ensure the safety, privacy, and confidentiality of medical records



## ➤ ABHA Registration

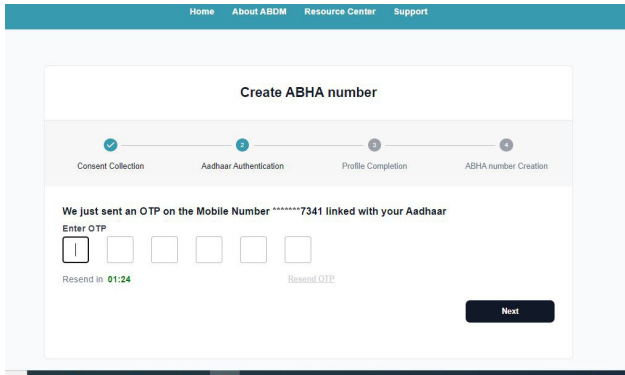
### ● Guide to create ABHA Number

1. Visit the Official Site : <https://healthid.ndhm.gov.in/register>

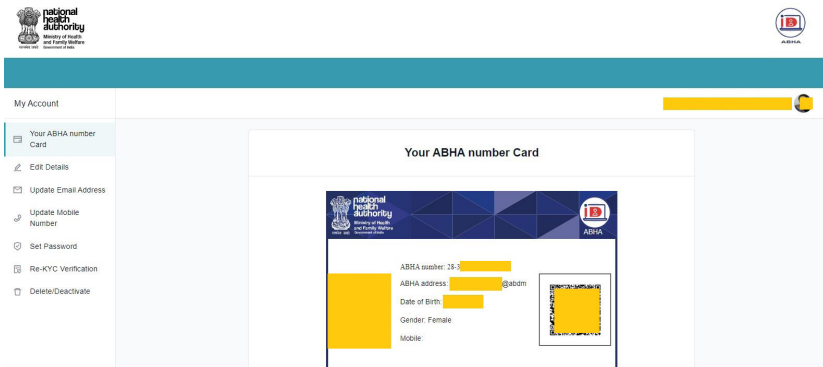
2. Select a option for ABHA number Creation (E.g: Using Aadhaar)

#### 2.1 Enter the Aadhaar Number

2. Enter OTP



3. Screen with ABHA card will appear.

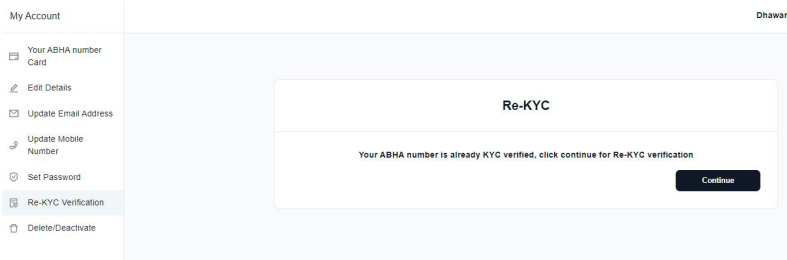


One can update Phone, Email Address and password from tab menus available in the My Account Screen.

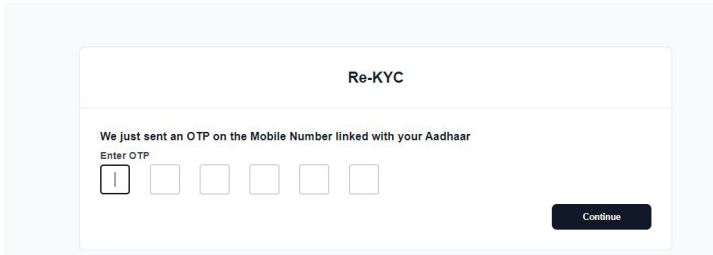
4. Add Phone No

5. Add Email No

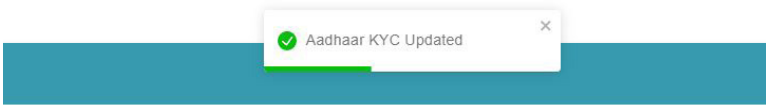
6. To Complete the KYC ,click on the KYC Verification tab and Click Continue.



7. Enter otp for KYC verification



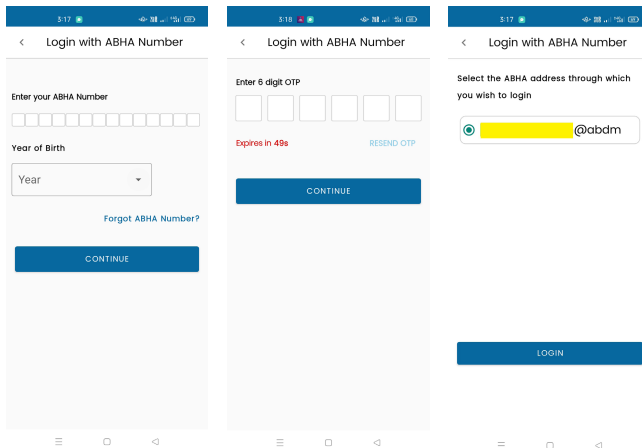
8. After successful KYC completion ,one will get the following popup.



Note: One can also delete or deactivate the ABHA account.

- **Guide to Link Health Locker with ABHA number**

Step 1: Login to ABHA app using ABHA number



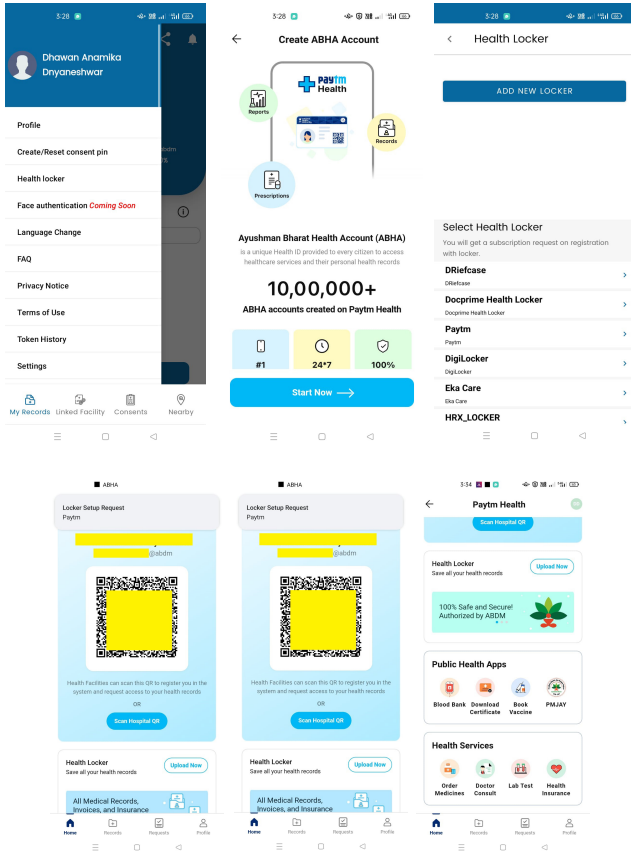
Step2 : After Successful Login Go to “Tab Menu Bar”

- 2.1. Select Health Locker.
- 2.2. Select add new Locker.
- 2.3. Select Paytm for example,You will get redirected to your paytm account
- 2.4. In Paytm app click Start now

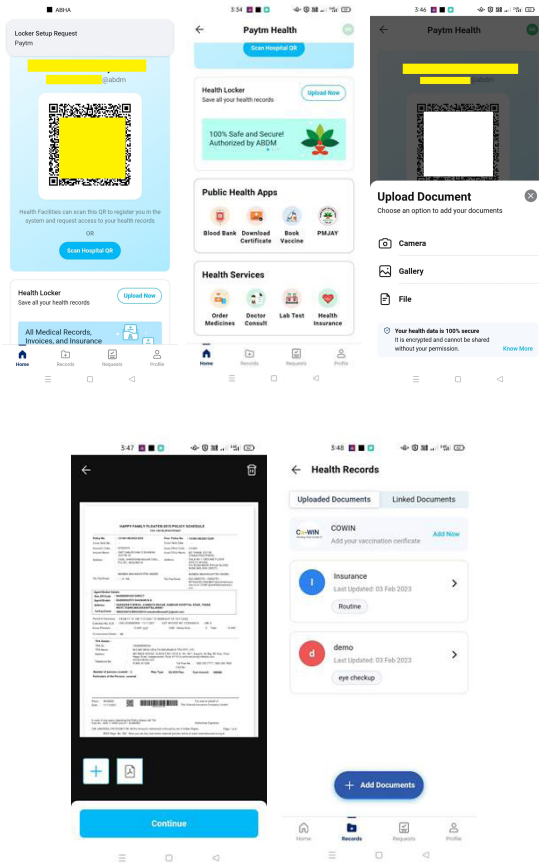
## 2.5. Verify Phone Number

2.6. Link ABHA number, A QR code will be generated there which will be used at health facilities to scan and request health records.

2.7. Upload Document in the Paytm ABHA locker, which can be viewed and edited later as well.







**Note:**Users can also check Requests to access his/her documents by healthcare facilities and approve or reject them from the Requests Menu.

- **Guide of ABHA healthcare Professional Registration**

1. Visit the Official Site: <https://hpr.abdm.gov.in/en/users/login>
2. Select New User creation.
3. Provide the Following Details:

**Welcome!**

To Ayushman Bharat Digital Mission  
Healthcare Professional Registry

Select your registration council  
Please select:

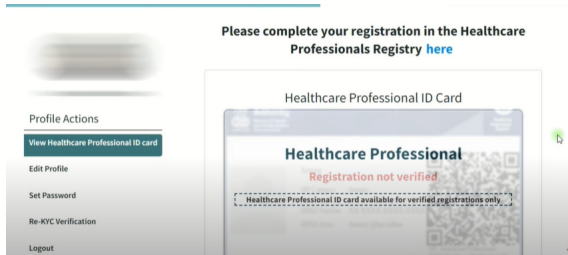
Enter registration number

Select Category  
Please select:

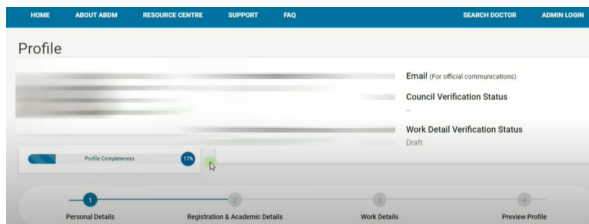
Select your Category  
Please select:

I'm not a robot

4. After valid credentials you will get redirected to my Account
5. Complete profile Details like Email, Phone No



6. Enter Registration Details



7. Enter Qualification details:

**Registration Details ( Ayurveda )**

Registered With Council \*

Registration Number \*

Registration Date (if available)

Is this registration permanent or renewable?\*

Permanent  Renewable

Due date of renewal

Registration Certificate Attachment \*

No file chosen

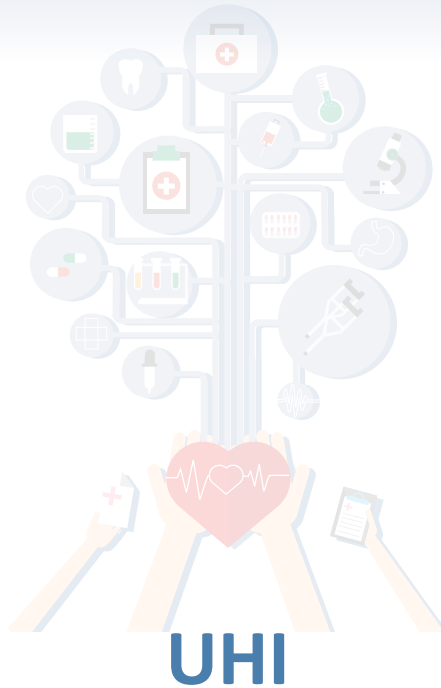
Max Allowed File Size 1 MB. (Allowed Formats : PDF, PNG, JPEG, JPG)

Is your name in registration certificate, different from your name in Aadhaar?

Yes  No

**Qualification Details ( Ayurveda )**

# 3








## ➤ **What is UHI?**

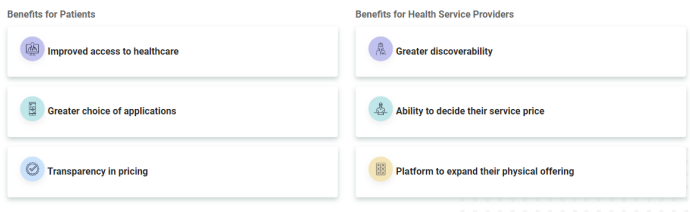
Interoperability in health services is made possible via a network of open protocols called the Unified Health Interface (UHI). The Ayushman Bharat Digital Mission (ABDM) Stack, which focuses on the accessibility and provision of health services, includes UHI as one of its fundamental layers. UHI makes use of the existing ABDM building blocks to give consumers a smooth end-to-end experience, enabling the interoperable sharing of personal health data as well as registries for physicians, patients, and healthcare institutions. Through UHI enabled applications, patients can discover, book, conduct and pay for services offered by a variety of participating providers from any application of their choice

## ➤ UHI Services

The following services are provided:

<p><b>1. Teleconsultation</b></p>  <p><b>Teleconsultation</b> Book an online consultation with any doctor</p>	<p><b>2. Booking Appointments</b></p>  <p><b>Booking Physical Appointments</b> Book your physical appointment with any doctor</p>	<p><b>3. Blood Donation</b></p>  <p><b>Blood Donation</b> Find a blood bank near you</p>
<p><b>4. Lab Bookings</b></p>  <p><b>Lab Bookings</b> Lab tests at your doorstep</p>	<p><b>5. Ambulance Booking</b></p>  <p><b>Ambulance Services</b> Book an ambulance pick up or a drop</p>	

## ➤ Benefits of UHI



## ➤ Stakeholders

### ● Citizen : Health ID

UHI will increase accessibility, quality, and efficiency by allowing end users / patients to access many digital health services from any platform of their choosing. Additionally, patients will be able to view and share their electronic medical and health information with the healthcare professionals of their choice, including medical reports, test findings, clinical records, etc.

### ● Healthcare Services : Healthcare Facility Register

The adoption of UHI is predicted from healthcare providers. HSPs include, but are not limited to:

- Doctors of any system of medicine
- Hospitals
- Labs
- Pharmacies
- Health service aggregators (platform players that partner with various health organizations to offer services to end users)
- Home care providers (including home nursing care, teleconsultations, and labs offering home sample collection services)

## ● Technology Service Providers

Technology service providers are businesses that provide patients and health care providers software interfaces that are UHI-compatible, making them the third major participant in the UHI ecosystem. These programmes implement UHI protocols to make it possible to give digital health services. TSPs must adhere to all UHI-defined protocols, certifications, and rules. On the UHI network, only approved apps can register and access services.

## ➤ UHI Sandbox

The sandbox environment, which is hosted on the ABDM infrastructure, offers a ready-to-use integrated environment with installed and provided core/foundational services.

ABDM is in charge of managing all hosted services and applications. Once the ABDM Sandbox team has contacted you, you may register your system via APIs or use the already-existing infrastructure components to create your own applications or integrations. The API endpoints for each of the separate components and services are listed below.

The following services are exposed publicly. In order to test the sandbox application, you will need to connect to your respective applications via API.

Application name	API Base URL	Description
ABHA Number Service	To be updated	Health Account Service
HFR	To be updated	Health Facility Registry
DigiDoctor	To be updated	Doctor's Registry
HDCM	<a href="https://dev.ndhm.gov.in/devservice/cm">https://dev.ndhm.gov.in/devservice/cm</a>	Consent-Manager
Gateway	<a href="https://dev.ndhm.gov.in/devservice/gateway">https://dev.ndhm.gov.in/devservice/gateway</a>	Gateway
HIU API	<a href="https://dev.ndhm.gov.in/devservice/hiu-api">https://dev.ndhm.gov.in/devservice/hiu-api</a>	Health information user
Example HIP	<a href="https://dev.ndhm.gov.in/devservice/hip">https://dev.ndhm.gov.in/devservice/hip</a>	Health information provider
HIU Web Interface	<a href="https://dev.ndhm.gov.in/devservice/hiu">https://dev.ndhm.gov.in/devservice/hiu</a>	HIU Website
Developer Service API	<a href="https://dev.ndhm.gov.in/devservice/devservice">https://dev.ndhm.gov.in/devservice/devservice</a>	Developer self service APIs

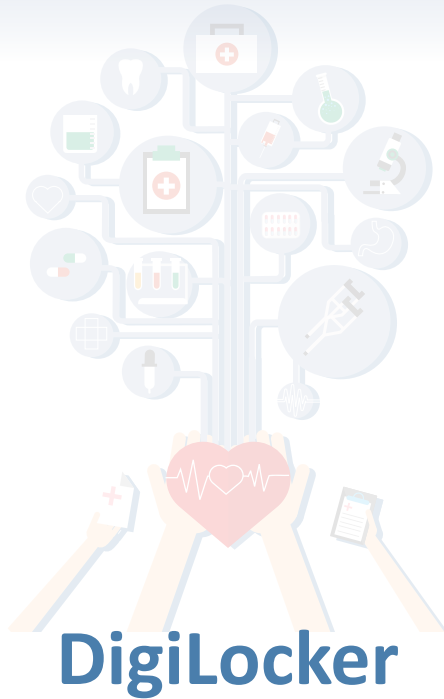
## ● Building UHI EUA App

This details out the steps to build your own EUA app including

- Sign up / Sign in with PHR Address
- Select a UHI service

- Teleconsultations
  - Search HSPAs for Doctor
  - Display search results
  - Book selected Doctor/Facility
  - Collect Payment if required
  - Confirm Booking
  - Exchange Messages with Doctor
  - Share health records
  - Setup WebRTC (teleconsults)
  - Initiate Call (teleconsults)
  - Get final prescription
- Appointment booking
  - Search HSPAs for Facility/Doctor
  - Display search results
  - Book selected Facility/Doctor
  - Collect Payment if required
  - Confirm Booking
- Ambulance booking
  - Search HSPAs for Facility/Doctor
  - Display search results
  - Book selected Facility/Doctor
  - Collect Payment if required
  - Confirm Booking

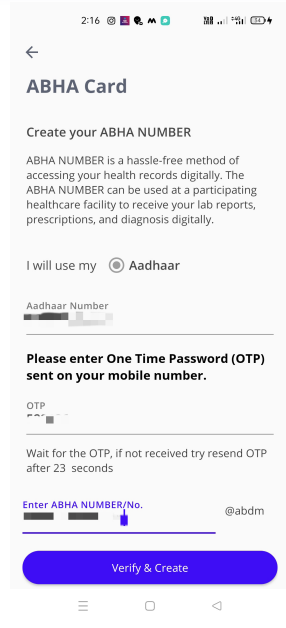
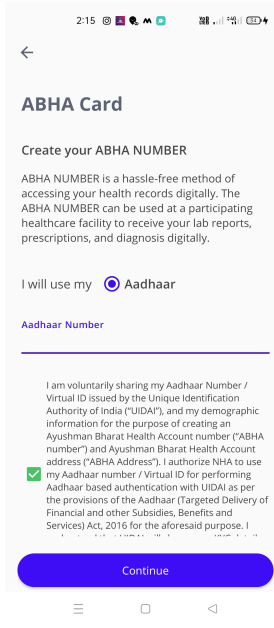
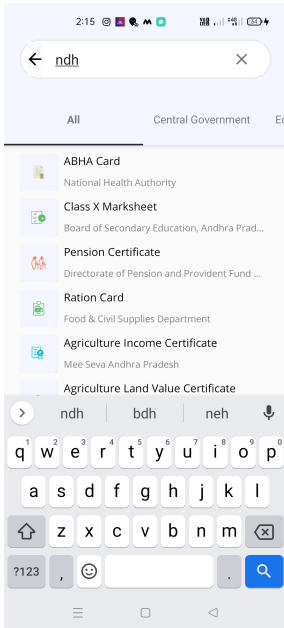
# 4



A simple and Secure Document wallet. It aims at 'Digital Empowerment' of people by providing them access to their authenticated digital document wallet. DigiLocker targeted the idea of a platform which will let issuance and verification of documents and certificates for Indian citizens, therefore making a paperless governance. Documents in the wallet (Aadhar card, Fitness Certificate, etc) are considered as valid identity proof at Indian Railways and Airports.

➤ **ABHA Card generation in DigiLocker.**

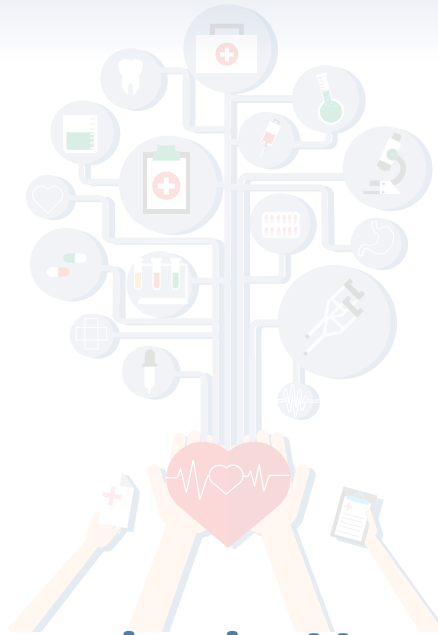
1. Open DigiLocker using Aadhaar Credentials
2. Search for ndhm
3. Select ABHA card
4. Enter Aadhaar Number and user will get OTP on registered Mobile Number
5. Provide a Name for ABHA number and Save



Now ABHA Card will be added to DigiLocker.



# 5



## Cybersecurity in Healthcare : The Foundation for Digital Transformation

The world we live in is a network like a mesh including our finances, social profile and governmental infrastructure. Cyber security by default has become a necessity. Cyber security encompasses everything from protecting personal information to intellectual property from deliberate attempts of damage and theft risks are festering as the world leans more towards cloud services and global connectivity. For example facebook had a security breach where hundreds of millions of facebook user records were exposed on amazon cloud server.

According to content delivery network provider akamai gaming industry has been the biggest victim of cyber attacks in the past couple of years

### ➤ **What is Cyber Security in Healthcare?**

Cyber security cyber security is a practice of protecting systems and networks from digital attacks.

Healthcare organizations use multiple health monitoring systems such as EHR programs, radiology information systems, practice management systems, e-doctor systems, clinical support systems, and physician programs. Patient admissions, prescriptions, pharmacy, and insurance are all a part of healthcare digitization now.

As we leverage and accelerate the adoption of digital technology in all domains and workflow, we can also notice the difference between the working methods efficiency and productivity of work being done. These changes can also be seen in the field of healthcare organization. With the embracement of technology medical science has achieved great success but as the saying goes that every pro comes with its own set of cons.



Figure 1 : Traditional technology vs Digital technology in healthcare



*Now Everything is Digital...*

Digital transformation means that healthcare organizations are now moving to the Cloud and adopting new technologies, such as connected medical devices, and paving the way to precision medicine. Cybersecurity solutions must keep pace with the healthcare providers and payers' innovation so they can operate with complete trust. They face challenges complying with tightening regulations; they're constantly combating increased cyber risks and adapting to digital transformation. The field of healthcare right now is very dynamic. It's really not if a breach happens it's really where we all know that health care institutions are very vulnerable. They're vulnerable because of a number of different things. This is an exciting time in healthcare because healthcare is changing and new technologies are being developed daily that allow patients to track their own health.

## ● Healthcare Stakeholder

Stakeholders in healthcare can include but are not limited to, patients, caregivers, doctors, nurses, unions, employees, employers, government, insurance companies, communities and pharmaceutical firms.

A stakeholder is an individual, or group of people, that all share a common interest in a project or organization, and share an interest in its outcomes.

Let's take a hospital as an example, there are multiple stakeholders for a hospital including:

- Patients, community, pharmacies, doctors, nurses and even charities.
- Another slightly different example is an elderly care home. An elderly care home would identify its stakeholders as patients, family members, community and maybe even funeral parlours.
- Stakeholders in healthcare will include primary and secondary stakeholders. The primary stakeholders in a hospital would be the doctors and the secondary stakeholders may be the pharmaceutical companies.
- A secondary stakeholder is a stakeholder who may disrupt or affect the relationships with the primary stakeholders.

Why Healthcare Gets Hit More ...???

What Makes Healthcare a Prime Target...???



## ● Patients

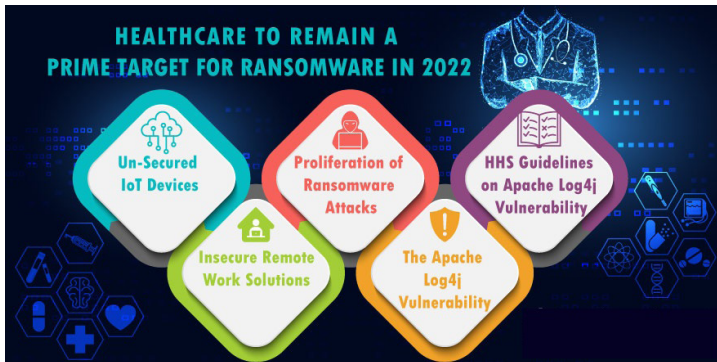
Patients need to understand how they securely communicate with healthcare providers. Additionally, if patients engage virtually with their healthcare providers, whether through telehealth platforms or other virtual meeting platforms like zoom, skype etc. Patients need to understand the privacy and security policies and also how to keep their information private and secure.

Healthcare organizations are particularly vulnerable and targeted by cyberattacks because they possess so much information of high monetary and intelligence value to cyber thieves and nation state actors. The targeted data includes patients' protected health information, financial information like credit card and bank account numbers.

Personally identifying information such as social security numbers and intellectual properties related to medical research and innovation.

Few years back firewalls and antivirus softwares were used as security measures but that is not the case now we have stepped into a new phase in this digital world where cyber crimes are increasing rapidly with the advancement in technology. Cyber security plays a major role in securing data from data breaches in various organizations. Data breach is nothing but stealing information from an organization system without the consent of the owner.

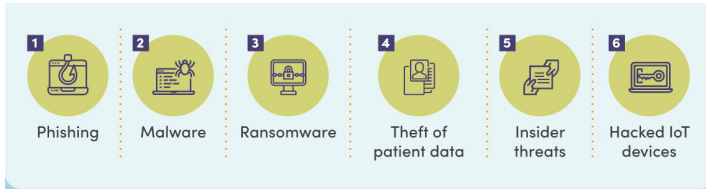
Let's answer the former first but before that you all should know what are the ransomware attacks Ransomware attack is a form of malware that when downloaded to a device deletes all data.



● **Why Healthcare Is A Prime Target for Cyber Criminals...?**

1. Patient information is very valuable
2. Healthcare has a broad attack surface
3. Hospitals use outdated technology and legacy systems
4. Limited training opportunities
5. Healthcare cyber-attacks can cause chaos
6. The digitization of health records
7. Ransomware is more profitable when lives are at stake: Ransomware attacks are pointless if nobody is willing to pay the ransom. However, in a life or death situation, hospitals may be left with no choice but to pay, should they get infected.

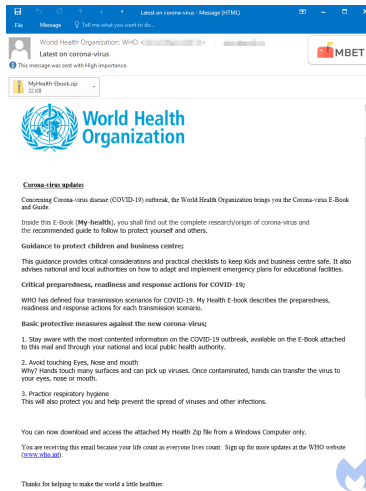
## ➤ Biggest Cyber Threats in Healthcare



Healthcare organizations can expect ransomware, botnets, cloud misconfigurations, web application attacks, and phishing to be their top risks.

### ● Phishing

- Phishing is the practice of infecting a seemingly innocuous email with malicious links. The most common type of phishing is email phishing.
- Phishing emails can look very convincing, and they usually reference a well-known medical disturbance to incentivize link clicking.
- Here's an example of a phishing email posing as a message from the World Health Organization.



- Phishing is the most prevalent cybersecurity threat in healthcare. Once again, a lot of the phishing activity targeting the healthcare sector over the past year has been related to the COVID-19 pandemic.
- India ranked third globally and first in the Asia-Pacific region in the list of 111 countries affected by a world-wide cyberattack involving a syndicate of cybercriminals stealing passwords through a concerted phishing campaign, according to a recent report

- An analysis that researchers at Palo Alto Networks Unit42 team conducted recently showed a 189% increase in phishing attacks relating to or targeting pharmacies and hospitals just between December 2020 and February 2021. Vaccine-related phishing attacks soared 530% over the same period.

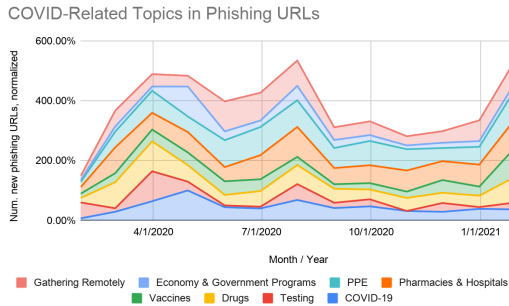


Figure 1. Trends in COVID-themed phishing attacks from January 2020-February 2021 (global).

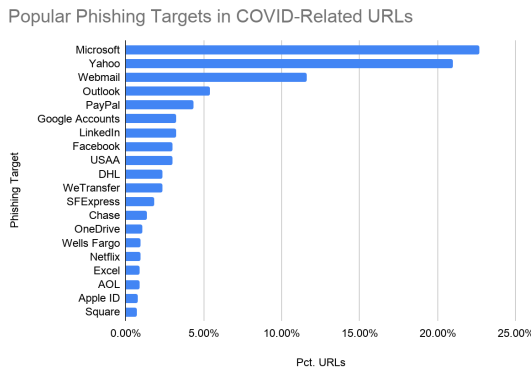


Figure 2. Top phishing targets in COVID-related URLs (global). Each bar represents the percentage of phishing URLs attempting to steal users' login credentials for that particular website. (Note that in this figure, we only include URLs that target identifiable brands.)

### How to Prevent Healthcare Phishing Attacks

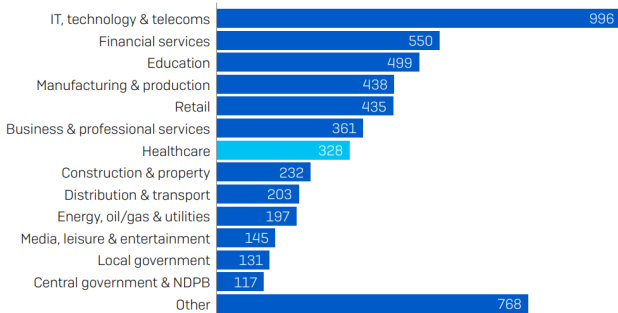
- To combat phishing, a combination of measures are required, which should include an email security solution to prevent phishing emails from reaching inboxes, a web filter for blocking access to phishing and other malicious websites, antivirus software on all endpoints, an intrusion detection system for identifying suspicious activity, and comprehensive security awareness training for the workforce to raise awareness of the threat of phishing, along with phishing simulations for testing the resilience of the workforce to phishing attacks.

- To limit the harm caused should an attack result in credential theft, multi-factor authentication should be used on all email accounts.
- It is also important to clear email accounts regularly so that if an account is compromised, the amount of data that can be obtained will be minimized. Since emails may need to be retained for legal reasons, consider using a secure email archive.

## ● Ransomware

- Ransomware is a type of malware attack in which the attacker locks and encrypts the victim’s data, important files and then demands a payment to unlock and decrypt the data.
- This type of attack takes advantage of human, system, network, and software vulnerabilities to infect the victim’s device—which can be a computer, printer, smartphone, wearable, point-of-sale (POS) terminal, or other endpoint.
- During a ransomware attack, malware is injected into a network to infect and encrypt sensitive data until a ransom amount is paid. This malicious software is usually injected into a system through a phishing attack.
- Ransomware attacks are a growing threat amongst healthcare providers according to an analysis last year. More than 1 in 3 healthcare organizations globally fell victim to a ransomware attack in 2020.

Within which sector is your organization? [5,400]



## Key Findings

- 34% of healthcare organizations were hit by ransomware in the last year.
- 65% that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack.
- 44% of those whose data was encrypted used backups to restore data.

- 34% of those whose data was encrypted paid the ransom to get their data back in the most significant ransomware attack.
- However, on average, only 69% of the encrypted data was restored after the ransom was paid\*
- 89% of healthcare organizations have a malware incident recovery plan



Hit by ransomware in the last year



Not hit by ransomware in the last year, but expect to be hit in the future



Not hit by ransomware in the last year, and don't expect to be hit in the future

In the last year, has your organization been hit by ransomware? [328 healthcare respondents]

- **How to detect and prevent Ransomware :**

1. Proactively monitor your server, network, and back up key systems.
2. Keep your operating system patched and up to date.
3. Educate your end-users about malicious spam and creating strong passwords.
4. Invest in dependable cybersecurity technology.

➤ **Healthcare Data Breaches**

List of some of the biggest data breaches in the healthcare industry

**1. Aadhaar Data Breach**



**Date: March 2018**

**Impact: 1.1 billion people**

In March of 2018, it became public that the personal information of more than a billion Indian citizens stored in the world's largest biometric database could be bought online.

This massive data breach was the result of a data leak on a system run by a state-owned utility company. The breach allowed access to private information of Aadhaar holders, exposing their names, their unique 12-digit identity numbers, and their bank details.

The type of information exposed included the photographs, thumbprints, retina scans and other identifying details of nearly every Indian citizen.



## 2. Yahoo Data Breach (2017)



**Date: October 2017**

**Impact: 3 billion accounts**

Yahoo disclosed that a breach in August 2013 by a group of hackers had compromised 1 billion accounts. In this instance, security questions and answers were also compromised, increasing the risk of identity theft. The breach was first reported by Yahoo while in negotiations to sell itself to Verizon, on December 14, 2016. Yahoo forced all affected users to change passwords and to reenter any unencrypted security questions and answers to re-encrypt them.

## 3. Tricare Data Breach



**Date: September 2011**

**Impact: 5 million patients**

**How did the breach occur?**

Tricare, a healthcare program servicing active-duty troops, their dependents, and military retirees, suffered a significant data breach following the theft of backup tapes of electronic health records. The backups were stolen from the car of an individual responsible for transporting the tapes between facilities.

It's unclear whether the criminals possessed the necessary acumen to decrypt the information stored on the tapes, or if they understood what they were stealing.

**The following data may have been compromised in the Tricare data breach:**

- Social security numbers
- Names
- Addresses
- Phone numbers
- Personal health data
- Clinical notes
- Lab tests
- Prescription information

#### 4. Community Health Systems Data Breach



**Date: April-June 2014**

**Impact: 4.5 million patients**

**How did the breach occur?**

Cybercriminals believed to be located in China, exploited a software vulnerability by deploying high-sophisticated malware leading to the theft of sensitive patient data. The incident impacted anyone that received treatment from a facility associated with the community health system network in the last 5 years.

The following information was compromised in the Community Health System data breach:

- Names
- Birth dates
- Social Security numbers
- Phone numbers
- Addresses

#### 5. Medical Informatics Engineering Data Breach



**Date: July 2015**

**Impact: 3.9 million patients**

**How did the data breach occur?**

Medical Informatics Engineering (MIE), a developer of electronic medical record software, suffered a data breach impacting at least 11 of its healthcare provider clients. Cybercriminals accessed one of MIE's servers by using a compromised username and password and maintained undetected access for 19 days. 239 of MIE's clients were impacted by the breach.

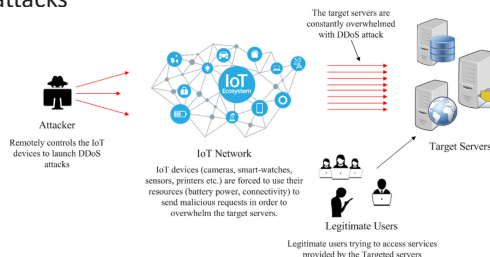
The following data may have been compromised in the Medical Informatics Engineering data breach:

- Names
- Telephone numbers
- Mailing addresses
- Usernames
- Hashed passwords
- Security questions and answers
- Spousal information
- Email addresses
- Dates of birth
- Social security numbers
- Lab results
- Health insurance policy information
- Diagnosis
- Disability codes
- Doctor names
- Medical conditions
- Names of children
- Birth statistics

## ● DDoS Attacks

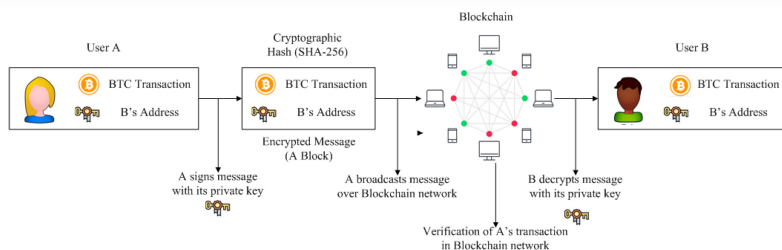
A Distributed-Denial-of-Service attack is a flood of fake connection requests directed at a targeted server, forcing it offline. During this attack, multiple endpoints and IoT devices are forcibly recruited in a botnet via a malware infection to participate in this coordinated attack.

Internet of Things (IoT) devices are widely used in many industries including smart cities, smart agriculture, smart medical, smart logistics, etc. However, Distributed Denial of Service (DDoS) attacks pose a serious threat to the security of IoT. Attackers can easily exploit the vulnerabilities of IoT devices and control them as part of botnets to launch DDoS attacks



*Fig : A DDoS attack scenario in IoT networks as a Botnet to target legitimate servers.*

An important feature of Blockchain is the signing and verification process of the transactions that are carried out using Digital Signature, which is used to identify users with (owning) a pair of Public and Private Keys. When a user A wants to sign a transaction (e.g., transaction data in the form of sending crypto BTC), she first generates a Hash value derived from a transaction; then, she signs (i.e., encrypts) this Hash value using her Private Key and sends it to user B along with original transaction data. User B verifies this transaction by comparing the decrypted Hash (while using A's Public Key) and the Hash value derived from the received data using the same Hash function as A's; an example scenario is shown in figure.



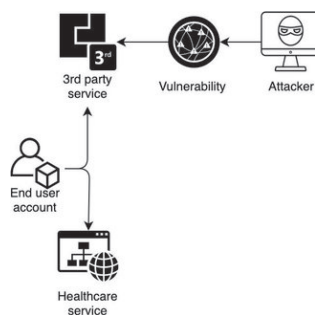
*Fig : The signing and verification of messages (i.e., transaction data) in a Blockchain network.*

- **Hot: Attacks against conferencing software**

With the pandemic showing no signs of slowing down, many employees are remaining at home, communicating with colleagues over teleconferencing and videoconferencing software. James Globe, vice president of operations at the Center for Internet Security (CIS), says attacks against those services will continue to be a concern.

He says organizations need to adopt formal corporate policies and procedures for staffers to follow to combat threat actors trying to piggyback on a session to eavesdrop on conversations and to view presentations that might contain sensitive information.

Globe recommends that organizations take steps like scrubbing invitation lists, password-protecting video conferences, sending out passwords in a separate communication from the meeting invitation, having the moderator manually admit participants, and locking the meeting once it starts.



*Attack on Zoom software*

**Key numbers:**

More than 30% of companies reported an attack of their videoconferencing systems during 2021, according to the Acronis Cyber Readiness Report.

## ➤ **Cybersecurity in Healthcare Best Guidelines**

### ● **Risk Assessment**

In the context of the healthcare industry, a security risk assessment typically refers to an enterprise-wide assessment of the potential threats to sensitive information and systems including PHI. A healthcare security risk assessment includes an evaluation of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information and systems. A security risk assessment also assesses an organization's capabilities for preventing, detecting, and responding to cyberattacks.

A security risk assessment should address the following considerations at a minimum:

1. Sensitive information discovery: where is our patient information and other sensitive information (e.g. PHI, credit card data, intellectual property, financial information)?
2. Threats actors: who are the bad guys and how likely are they to interact with our environment?
3. Threat vectors: what are the bad things that can happen and how likely are they to occur?
4. Vulnerabilities: how exposed are we and what weaknesses or security holes exist in our environment?
5. Impact analysis: if we have a bad day, how bad of a day will it be?
6. Risk determination: what are the most pressing areas we need to address?
7. Corrective action planning: how do we fix what we found?

A security risk assessment should seek to identify all locations and functions where sensitive information including PHI is created, received, maintained, or transmitted by the organization.

**Example locations where PHI is commonly stored and managed by healthcare entities:**

- Databases
- Servers
- Endpoints
- Removable Media (e.g. USBs)
- Backups
- Email
- Printers/Paper/File Drawers

- Mobile Devices (e.g. Laptops, Tablets, & Phones)
- Web Portals
- IoT & Medical Devices
- Third-party Vendors and Hosted Solutions

### What tools and technologies can be used to support security risk assessments?

There are several technology options available for organizations to support the completion of their security risk assessments.

This is not an exhaustive list, but some examples include:

- OCR and HHS have made available the HHS Office of the National Coordinator Security Risk Assessment Tool
  - Governance, Risk, and Compliance (GRC) tools and software typically have security risk assessment workflow and reporting modules and functionality
  - CORL Technologies offers a platform and services for conducting third-party vendor security risk assessments
- **Security Controls**

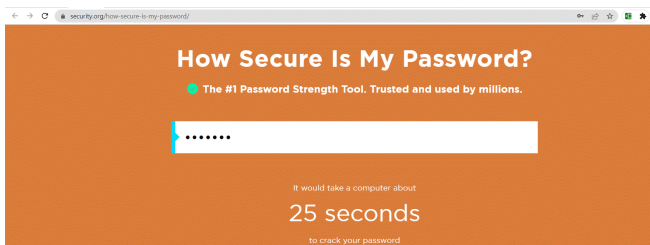
Cyber security attacks are becoming more and more common over time, so it's important to know what you can do to protect your information online. While there's no bulletproof way to prevent an attack, there are a lot of things you can do that will help to lessen the risk

- **How to secure the system ? ➤ What to do and what not to do...**

#### 1. Make a use of **STRONG PASSWORD**

To check How Secure Is My Password?

Visit following site : <https://howsecureismypassword.net/>



*Weak Password*



### *Strong Password*

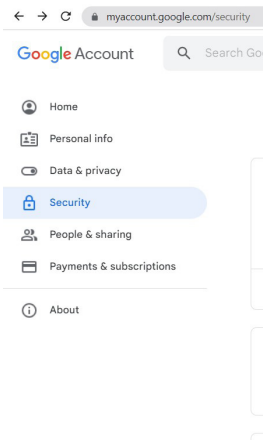
For Mobile Applications : Use Passphrase instead of passcode or pattern can be easily hacked

## 2. Turn on 2-Step Verification

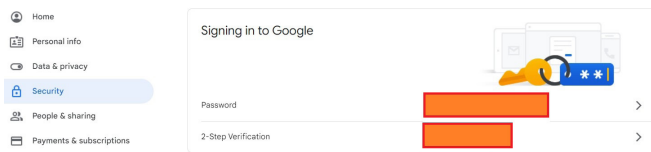
Steps to allow 2-Step Verification (Gmail)

### 2.1 Google prompts (Default)

1. Open your Google Account.
2. In the navigation panel, select Security.



3. Under “Signing in to Google,” select 2-Step Verification Get started.
4. Follow the on-screen steps.

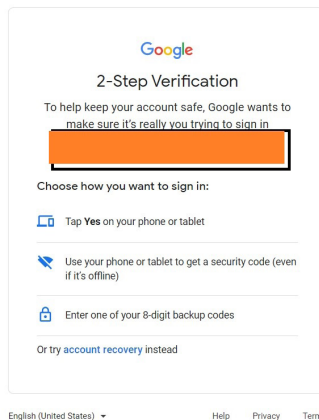
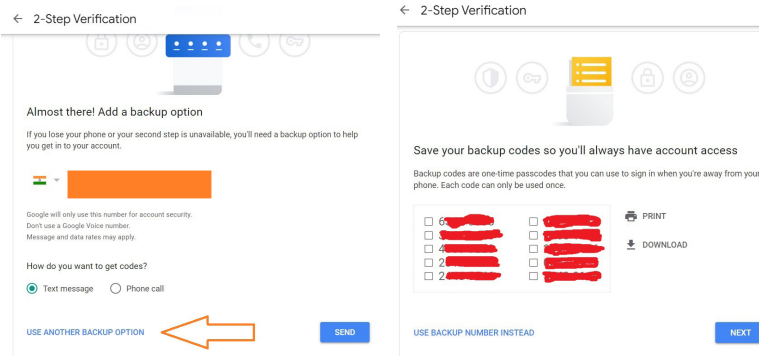


Tip: If you use an account through your work, school, or other group, these steps might not work. If you can't set up 2-Step Verification, contact your administrator for help.

## 2.2 Backup codes

9 single-use codes are active at this time, but you can generate more as needed.

Use Another Backup option ➤ Download one time password and used for login ➤ For Login time Choose third option given as “Enter one of your 8-digit backup code” given in following screen



## 3. Used Incognito Window.

Using incognito mode prevents any data or browsing history associated with a particular browsing session from being stored on your device. That means that anyone else using your device won't be able to see which websites you visited or what you searched for in Google

Is incognito safer? ➤ **It won't protect you from viruses or malware**

## 4. Use of VPN <https://www.itopvpn.com/>

VPN stands for “Virtual Private Network” and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your



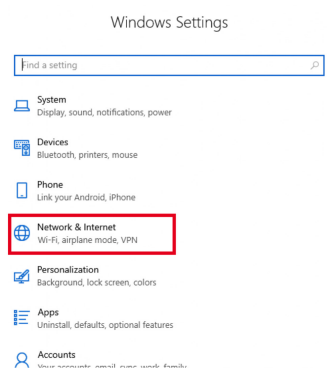
internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data.

Use VPN for following situation

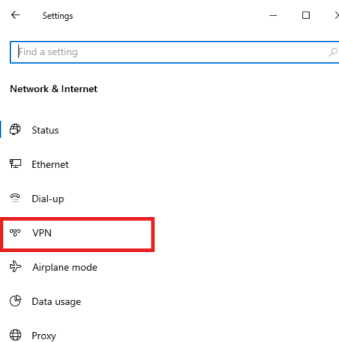
- Keep browsing activity private
- When you are using public wi-fi
- Accessing Sensitive information
- Reduce mobile data usage

### For Windows 10 S

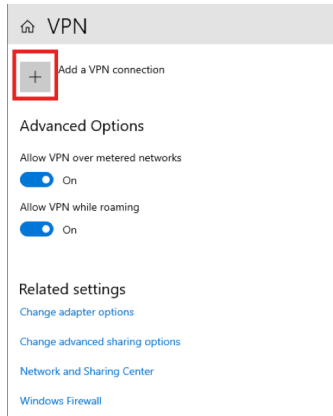
- Install the FortiClient from the Microsoft Store
- Go to the Windows Menu and select “Settings”
- In the Windows, Setting go to “Network & Internet”



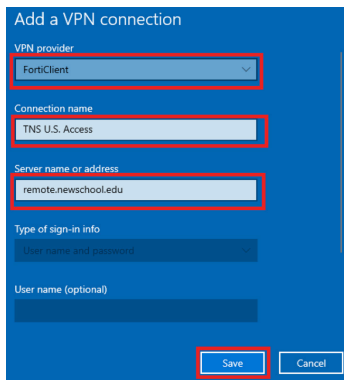
- In the Network & Internet and select “VPN”



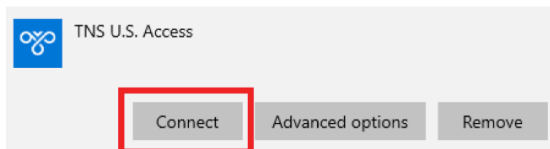
- In the VPN select “+” to add a VPN connection



- In the VPN provider Select “FortiClient”, Give the connection a name “TNS U.S. Access”, in the server name or address add “remote.newschool.edu” and “Save”

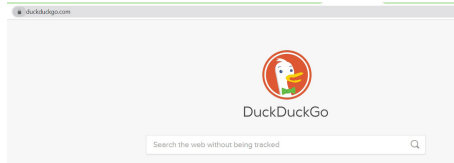


- To connect select “Connect”, you will get a login window for username and password, enter your NetID and Password.



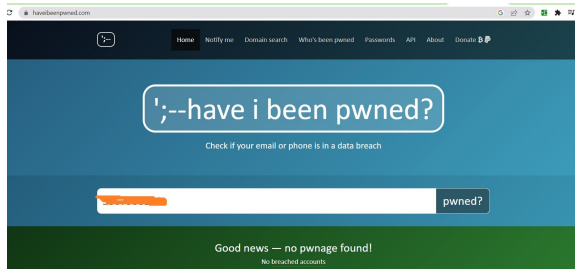
5. **Use of DuckDuckGo (Private browser) : <https://duckduckgo.com/>**

DuckDuckGo is a better option than Google or Bing. Statistics show that 80 million people have used the platform to access the internet, so it is clearly gaining traction. Over 35 billion queries were answered by this browser in 2021 alone.



6. **Check if your email or phone is in a data breach**

Open : <https://haveibeenpwned.com/>



7. **Always use 2-Mobile Number and 2- Gmail account**

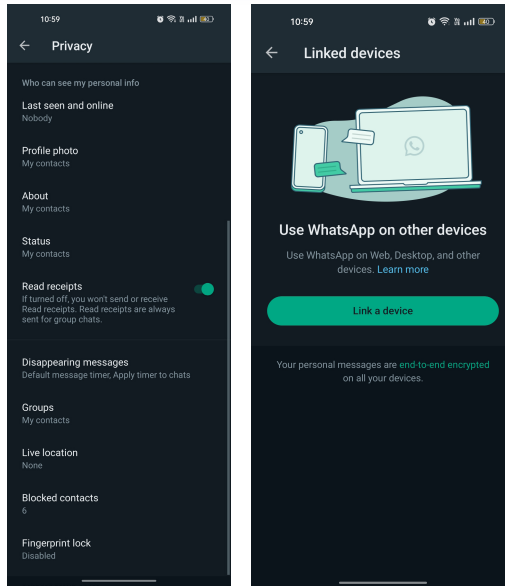
One for Personal things, linking to Addhar, banking purpose and second for others

8. **Do not share your personal information** like Photo, Aadhar card/PAN photo etc) publicly, not. even with friends and family. Do not share your information in any survey form, website or in any contest, status/stories on social media

9. Do not give your mobile to anyone for calling or any purpose. Spyware is used to hack your data from mobile.

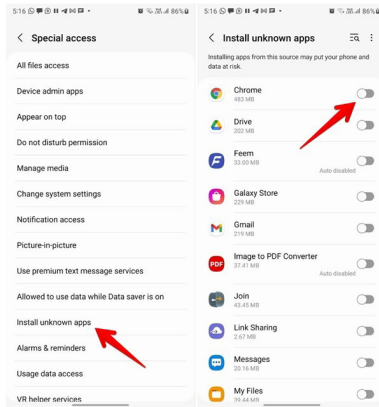
10. **Secure WhatsApp**

- Two-step verification
- Remove Linked Device
- Make all details as private



## 11. Do not download and install Third-party Apps

You can simply avoid this by disabling the unknown source app install option.



12. Another way to avoid being the victim of cybercrime is to **install anti-virus software and keep software up to date**, as updates generally upgrade security and remove bugs

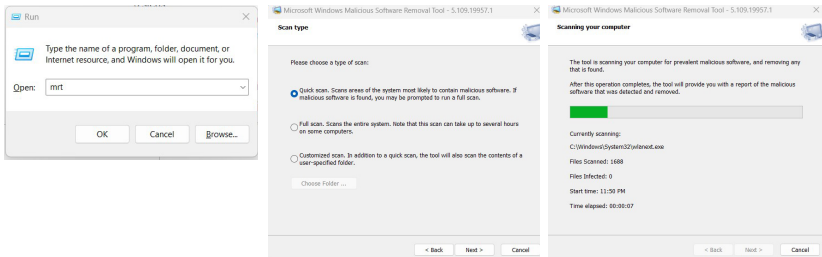
13. **Backup and restoration of files/data on Google drives constantly**

14. **Avoid to charge your mobiles/laptop on public spaces.** There are strong chances of PHISHING ATTACK ➤ Carry Power Bank



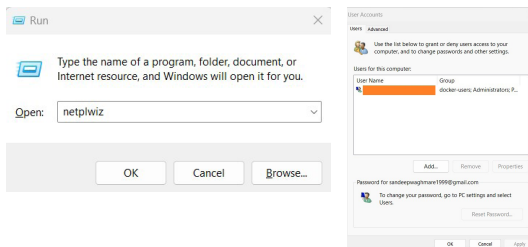
- 15. Stay off public networks and disable Bluetooth when not in use.
- 16. Never open suspicious emails or links.
- 17. Remove Virus from PC

Open Run using windows+R ➤ Type mrt and click Ok



- 18. Check website is secure or not from <https://www.urlvoid.com/>
- 19. Check if someone is spying on you ?

Press windows+R ➤ Type netplwiz and enter



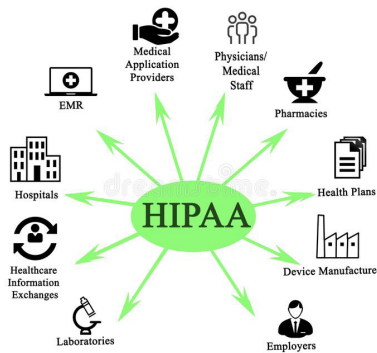
**20. Safe Browsing site status**

<https://transparencyreport.google.com/safe-browsing>

➤ **Cybersecurity in Healthcare Laws and Regulations**

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.



*Health Insurance Portability and Accountability Act of 1996 (HIPAA)*

**KEY TAKEAWAYS**

- HIPAA law impacts policies, technology, and record-keeping at medical facilities, health insurance companies, HMOs, and healthcare billing services.
- Noncompliance with HIPAA standards and best practices is against the law.
- The HITECH Act was created in 2009 to expand HIPAA privacy and security protections for patients.



## **How the Health Insurance Portability and Accountability Act (HIPAA) Works**

- The Health Insurance Portability and Accountability Act (HIPAA) ensures that individual health-care plans are accessible, portable and renewable, and it sets the standards and the methods for how medical data is shared across the U.S. health system in order to prevent fraud. It preempts state law (unless the state's regulations are more stringent).
- Since 1996, HIPAA has been modified to include processes for safely storing and sharing patient medical information electronically.<sup>2</sup> It also includes administrative simplification provisions, which are aimed at increasing efficiency and reducing administrative costs by establishing national standards.
- In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) broadened HIPAA privacy and security protections. The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009 as a way of promoting the use of health information technology. A portion of the HITECH Act addresses privacy and security concerns.

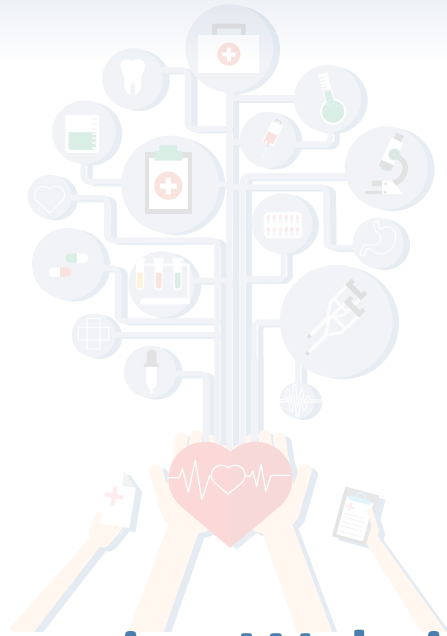
## **The Future of the Health Insurance Portability and Accountability Act (HIPAA)**

In 2018, Bloomberg Law reported on the privacy risks that come from digital healthcare data and the likelihood of updated federal laws in the near future.<sup>4</sup> In an age of fitness-tracking apps and GPS-tracked, shareable data on everything from an individual's daily step count to their average heart-rate, medications, allergies, and even menstrual cycles, there are new challenges for upholding standards in storing and protecting personal medical data.





# 6



## Converting Website to Mobile Application

- **Importance of Mobile Apps in Healthcare**

Healthcare-base mobile applications connect doctors with patients who need support, easing the burden on healthcare workers. For instance, Healthcare mobile apps offer 24x7 virtual assistance to patients by connecting them to certified doctors through calls, text, or video calls. It allows doctors to learn about their patient's symptoms and provide a digital prescription.



## **I. Improved Patient Engagement**

Studies have shown that a convenient and technology-driven healthcare experience can tremendously improve patient satisfaction.

Patient engagement focuses on making sure that patients and providers work together to improve the patient's health. In order to create patient engagement strategies that allow patients to become actively engaged in gathering information and making decisions about their symptoms, illnesses, and treatment options, providers need to empower the patient to have a voice in their healthcare experience.

## **II. Immediate Access to Care**

Extending the reach of patient care through connected technology means empowering providers to understand a patient's wellbeing in real-time and make confident decisions about the most appropriate care setting for each patient.

Considered a blessing for doctors, nurses, and other healthcare workers, the healthcare mobile application updates doctors about symptoms and ailing health conditions of the patient. These applications can be designed to check ailing symptoms and create a report.

## **III. Secure Payment Options**

Standing in a queue waiting to pay your medical bill is a thing of the past. With secure payment gateways integrated into healthcare mobile apps, bill payment becomes a hassle-free process. Highly secured payment gateway integration in the app facilitates users to make instant payments securely with a few clicks.

They can also select their preferred payment method, pay online (debit or credit card) and connect to their insurer (if required) via apps. Choose between your preferred payment mode (debit card, credit card, or mobile payment gateways like Paypal) to pay bills timely. Also, if you forget to make a payment, these apps will send a notification as a reminder.

## **IV. Real-Time Communication**

Apart from inspecting the patient's condition using high-definition cameras, mobile apps can also be used for real-time collaboration, consultation, and information sharing with doctors globally. This benefits the patients as doctors from across the globe can learn and share knowledge in real-time. Moreover, regular real-time communication between patients and doctors also improves monitoring by keeping a constant check on health.

## **V. Internet of things healthcare And Mobile Application**

The internet of things healthcare and mobile applications make the practice easy to gather patients' information and health data on IoT healthcare devices. The data

seamlessly flows via the connected medical equipment on patients' bodies meant for monitoring vital parameters.



The technology makes it easier to monitor the vital health parameters and alert the healthcare service provider when it exceeds the threshold value. IoT collaborates with medical and healthcare mobile apps delivering better care to patients while generating revenue opportunities for stakeholders. Moreover, with IoT, the treatment cost is also reduced significantly making it easier for patients to follow instructions.

## VI. HealthCare Apps are Blessing in far Remote Areas

Today's era of internet and with Smartphones reaching to every nook and corner, people living in rural areas can also expect to get the best health services. The on-demand apps help them to book appointments with doctors and buy medicines online without having to travel to the hospital.

In addition, they can also get information about important healthcare tips from time to time through push notifications.

These healthcare applications are a blessing in disguise as it is easy to book an appointment with the doctor along with purchasing medicines online too. Apart from that, push notifications are the easiest way to offer daily healthcare regimes and tips.

### ➤ How Mobile Apps can improve your business?

Mobile healthcare apps are transforming the healthcare ecosystem by improving communication, efficiency, and quality of the service.

Healthcare apps are a blessing to the medical industry. Not only doctors and patients, but hospital staff and pharmacists can also gain the benefits of this technological marvel. Mobile healthcare apps can be used for online consultation, diagnosis, appointments, and medical supply delivery.

The healthcare industry has witnessed enormous transformation due to technological advancement and interference. In the past few years, we can clearly see the role mobile app development has played in the transformation of the healthcare sector.

Following are the ways in which mobile apps can help you grow your business:

**I) Excellent Business Opportunity**

By offering digital solutions and making healthcare more accessible, mobile apps can help healthcare businesses increase patient satisfaction, reduce operational costs, and grow their patient base.

**II) Boost branding**

Healthcare apps help doctors, healthcare service providers build a brand, improve customer experience and increase profits in the long run.

If you want an instant brand boost or recognition, creating a mobile application is a great way to help improve your corporate branding and overall reputation.

**III) Digital Marketing acquire more patients**

By utilizing digital channels such as social media, email marketing, search engine optimization (SEO), and pay-per-click advertising (PPC), healthcare businesses can reach and engage with their target audience in a cost-effective and data-driven manner.

**IV) Enhancing patient data management and tracking of health information**

Enhancing patient data management and tracking of health information is one of the key benefits of mobile apps in healthcare. By digitizing and centralizing patient data, mobile apps can improve the accuracy and efficiency of healthcare delivery and support better patient outcomes.

**V) Greater flexibility and real-time adaptability**

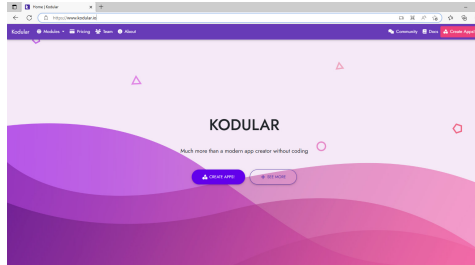
Greater flexibility and real-time adaptability are also benefits of healthcare mobile applications. This includes Real-time communication with patients and healthcare providers, On-demand access to health information and services, Personalized and adaptive features for individual patients, Integration with other healthcare technologies and systems.

By having the ability to quickly update and improve their mobile app, healthcare businesses can provide a better user experience, stay ahead of market trends, and deliver more effective and efficient care to their patients.

## ➤ Convert Website into Mobile Application

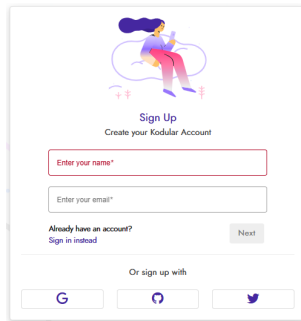
The fastest and most affordable way to build a mobile app is to convert your existing site into native mobile apps. Although web and mobile are two completely different platforms, there are still many shortcuts you can take advantage of to augment your web solution with a mobile app relatively quickly.

Let's Convert Website to App.

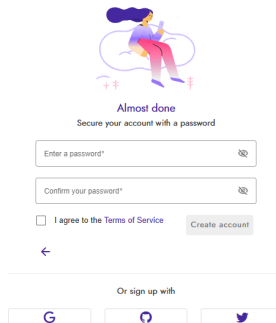


**Step: 1** Go to <https://www.kodular.io/>

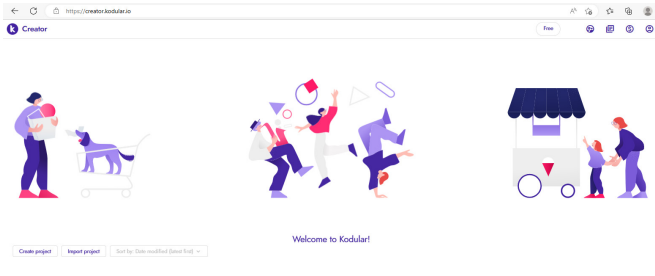
**Step: 2** Click on Create Apps and you will get Sign In form and Create Account Link. Being a new user you have to create an account. Enter your name and email address or sign up with gmail, github or twitter account.



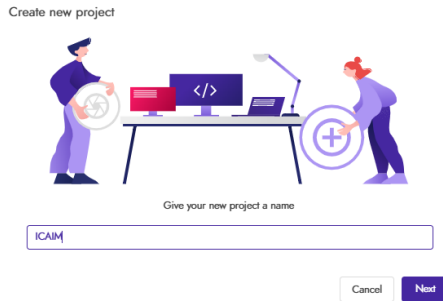
**Step: 3** Enter Password and confirm password and agree to the terms and conditions. And click on the Create Account button. After that you have to verify your email address and agree to the terms.



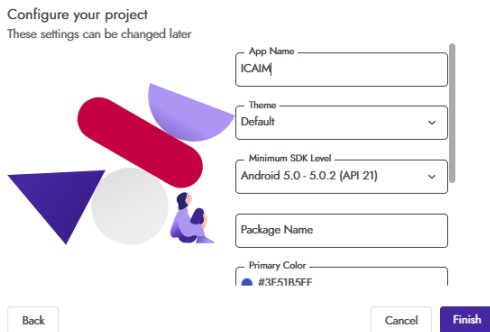
You will get the following screen after successfully login to the website. Click on Create Project Button.



**Step : 4** After clicking on Create new Project you have to provide Project Name and click on Next Button.



**Step : 5** In the Configure Project you have to provide the following information.



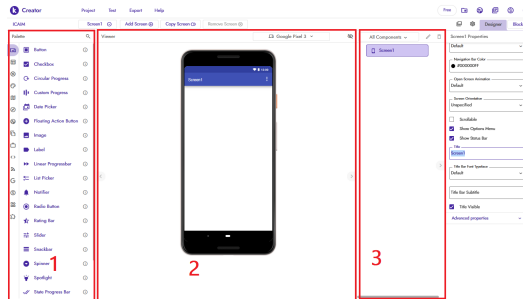
**App Name :** Name of Application

**Theme :** Select Application Theme (i.e. Light / Dark or Default)

**Minimum SDK :** Specifies the minimum API Level on which the application is able to run

**Package Name :** Enter unique package name

## Also Set Primary Color, Primary Color Dark and Accent Color which are the basic Application Colors



The above shown screen is called Designer.

From this page, you can add/delete **Components** and modify their properties.

1. On the left side of your page, numbered 1 is the **Components Palette** or simply Palette. This consists of various components grouped under different categories.

When you need to add a component, you can click on the component on the Palette, hold it and drag it onto the Viewer area of the Designer page.

2. On the right side, you have the **Components Hierarchy** and the Designer Properties Panel (which is visible when you select a component). The Components Hierarchy shows the visible components added into the current project. The Designer Properties Panel will be visible when clicking on a component and displays the properties of that component.

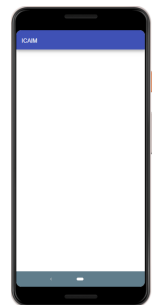
3. In the middle is the **Viewer** which gives a mocked up view of the app as seen on a real device. To add a component to the project, drag the component from the Palette and drop it inside the Viewer.

Below the Viewer, the **Non-visible Components** Panel is present, which shows all the Non-Visible Components added to the current project.

4. At the top of the page, various menus and options are present.

### Step 5: Change the Screen Properties

From the Screen Properties Window you can change the properties of your screen like the title and sub title of the screen. You can change the screen animation and orientation. You can also enable the scrollbar option and disable the show option menu and show status bar.

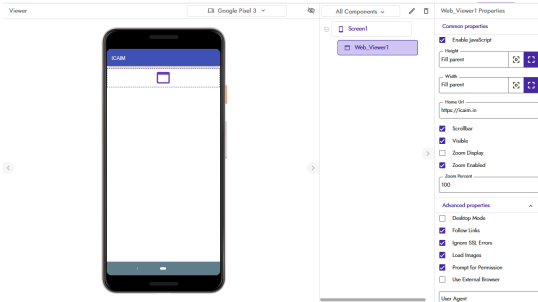


### Step 6: Getting WebView & Assigning URL

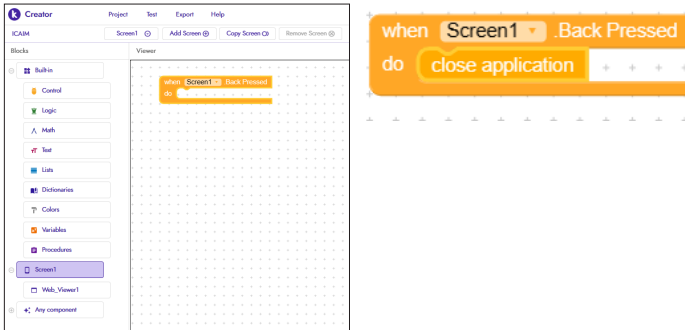
Drag & Drop the WebView Component in your App Screen into your project which could be found under the views subcategories under the Layout section in Components Pallet.

### Step 7: WebView Settings

Set the WebViewer's height & width to fill parent in properties section so that the WebViewer covers the full screen of the user's mobile device. Further, keep the "Zoom Enable" option in WebViewer's properties Disabled.



Add Home URL as your Website URL.



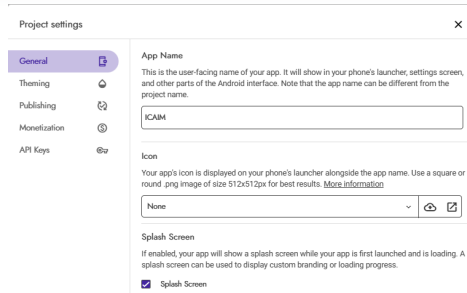
### Step 9 : Go to Screen 1 Block and select when Screen1.Back Pressed

And do the following. Close application is inside control block

### Step 10 : Project Settings

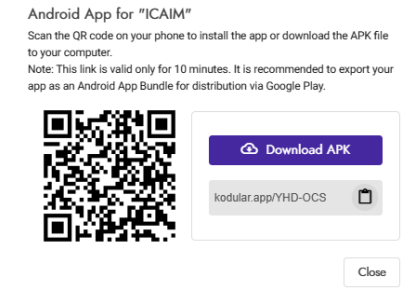
Inside Project Settings you can change the Application Icon and splash screen. Also change the primary colors of your application.



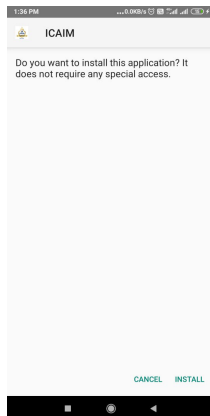


### Step 11 : Test and Export your Application

Select Export and click on Android APK (.apk). You can either scan the barcode or download the APK by clicking on the Download APK button.



Step 12 : Install APK and Open Application. You can now get your application with your name and logo.





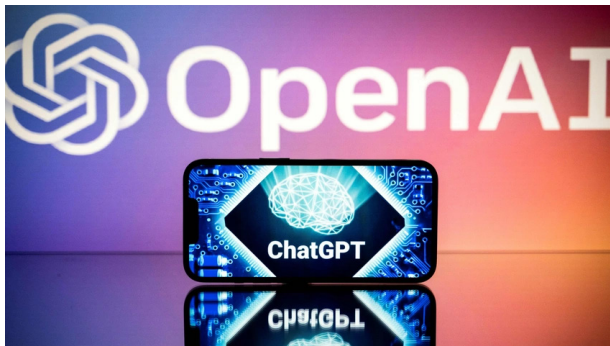
# 7



## Content Marketing - ChatGPT

### ➤ Open AI- ChatGPT

GPT stands for Generative, Pretrained, Transformer. ChatGPT can write emails and essays, poetry, answer questions, or generate lines of code based on a prompt. This could be used to develop virtual assistants or quickly answer customer queries. Content platform Jasper said about 80,000 clients have used its software to draft ads, emails, blogs and other material.

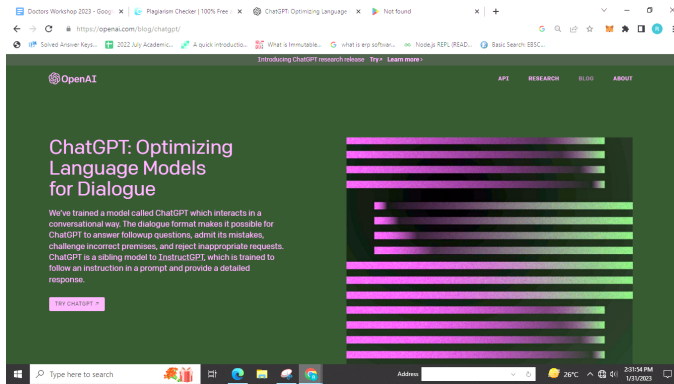


## ● Steps to use ChatGPT

The work for which you spend thousands of rupees, you spend lakhs of rupees, that work is also free and you do not need to watch YouTube videos, nor do you need to search Google for how to make a video or reel viral will know. You have to make any website, it will be ready withing a minute. If you want to solve a hard question of maths, then you will solve it in a minute.

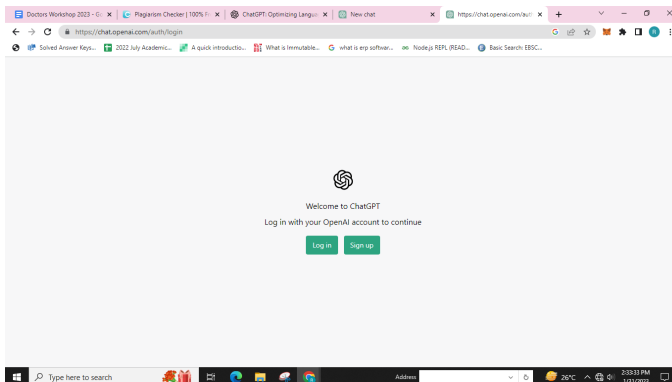
### How to create and account in ChatGPT

Step 1: open your browser and type in [chat.openai.com](https://chat.openai.com)

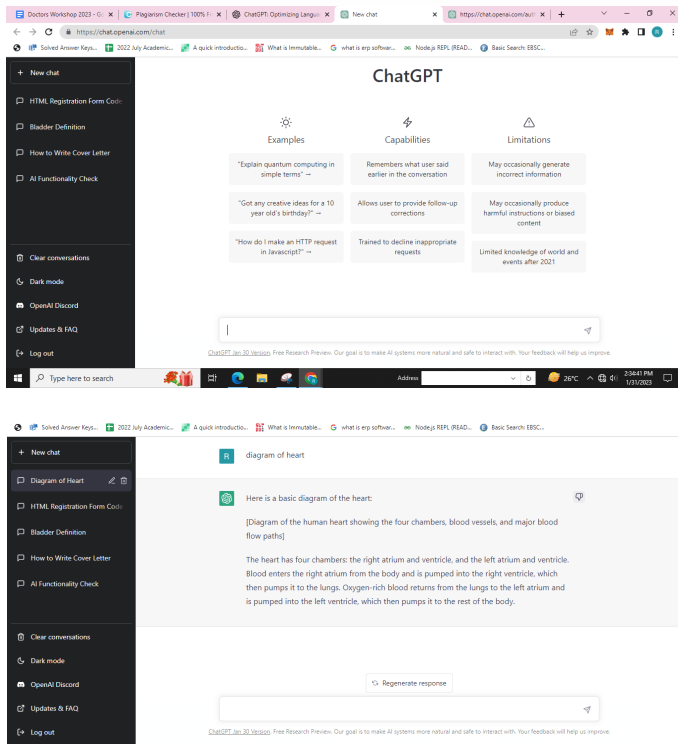


Step 2: click on “TRY CHATGPT”

Step 3: if you are existing user click on log in and for new user click on signup and fill the details. So account will be created.



Step 4: after log in to main window, where we can actually start typing and ask questions



This is how we can use this ChatGPT app

Now we will discuss some advantages and disadvantages

### ● Advantages:

1. **Natural language understanding:** ChatGPT can understand and respond to a wide range of human language inputs, making it useful for natural language processing tasks such as language translation, text summarization, and question answering.
2. **Human-like responses:** ChatGPT is trained on a large dataset of human-generated text, making its responses more human-like and natural than those generated by other models.
3. **Flexibility:** ChatGPT can be fine-tuned for specific tasks and industries, such as customer service or technical documentation, to improve its performance and make it more useful for specific applications.
4. **Efficiency:** ChatGPT can generate responses in real time, which allows for faster and more efficient communication.
5. **Cost-effective:** ChatGPT can automate many tasks that would otherwise require human labor, which can save time and money.

6. Scalability: It can handle multiple requests simultaneously, which can save time and money.

● **Disadvantages**

1. Reliability: At last its machine so sometime the given answer or data might be incorrect.
2. No multiple solutions: On google web search engine we got multiple option and where we can choice as based on query, as compared in GPT we don't get various option to verify the answer.
3. No Graphics availability: No diagrams, graphs can access on this.



