



# MEDICAL SOFTWARE DEVELOPMENT GUIDE GUIDE FOR MANAGERS

*By Nisos Health*



VOLUME I

---

# Medical Software Development Guide For Managers

---

---

**2021  
GUIDE**

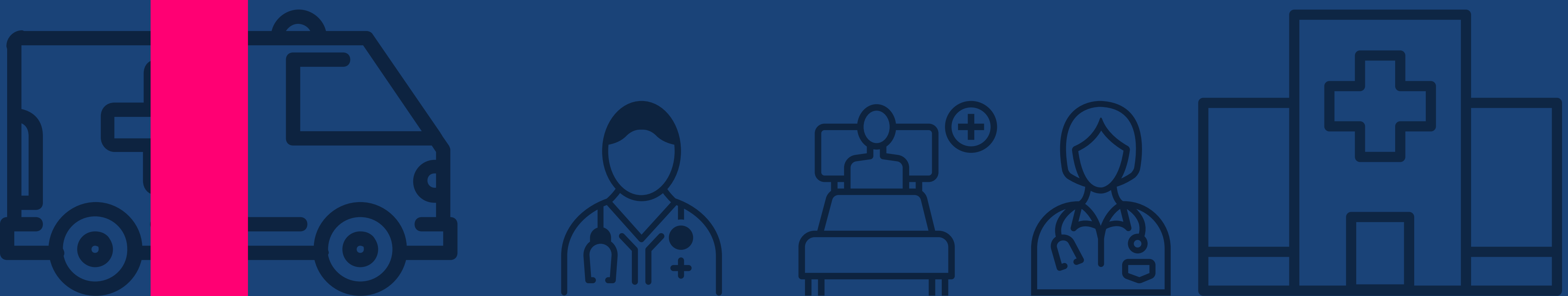
Written by Nisos Health (nisos.health)





# CONTENTS

- 04 Overview**
- 05 Top things to keep in mind during medical software development**
- 06 HIPAA compliance – what software developers need to know**
- 08 HIPAA secure messaging options in medical software development**
- 13 Chatbots to solve your social media and website communications**
- 16 HIPAA security of media being shared and stored**
- 17 Authentication and authorization of people using your platform**
- 19 Ability to integrate your EMR/EPM with the messaging platform**
- 21 HIPAA secure hosting and EMR integration**





Medical software development comes with its unique set of challenges. Most of them are related to EMR integrations, HIPAA compliance, HITRUST certification (if you are a software vendor) and the latest – cloud based healthcare software development.





# OVERVIEW

Medical software development comes with its unique set of challenges. Most of them are related to EMR integrations, HIPAA compliance, HITRUST certification (if you are a software vendor) and the latest – cloud based healthcare software development.

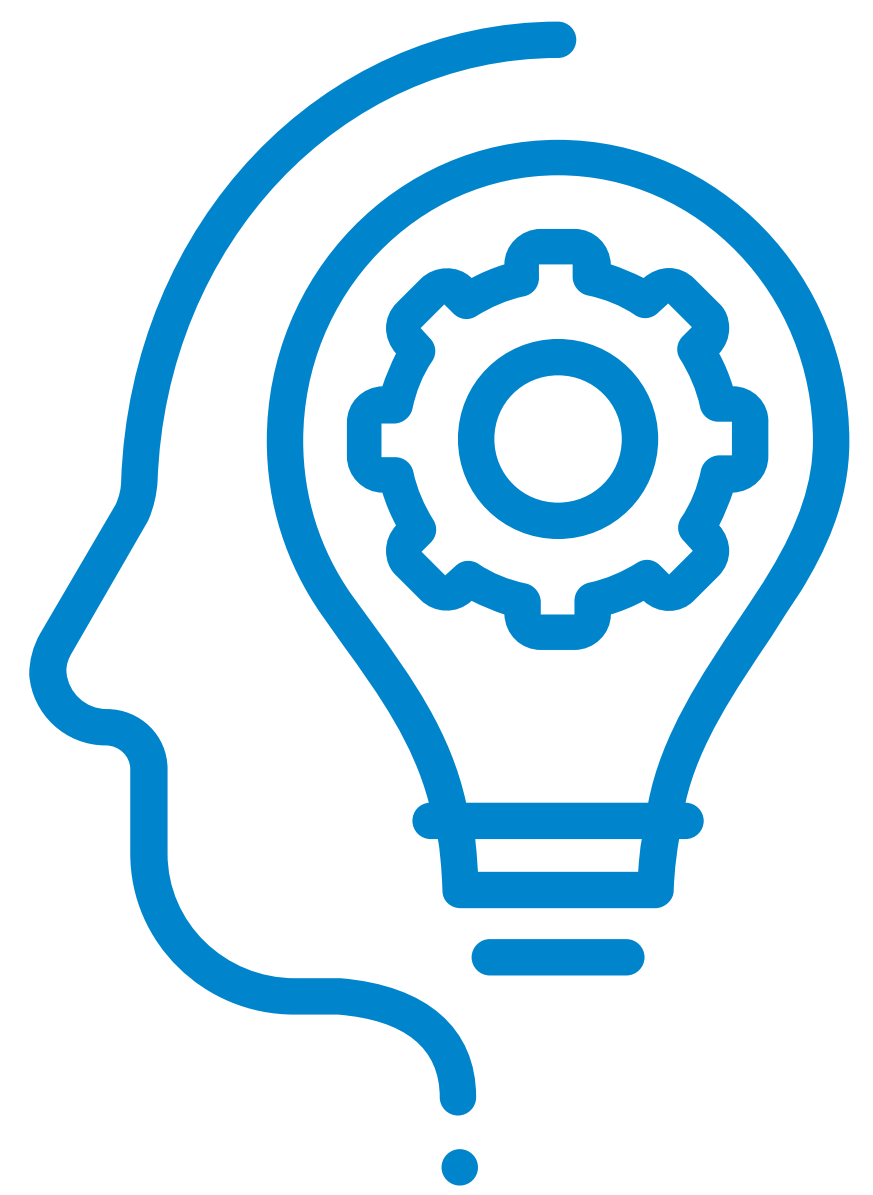
Considering that we provide healthcare IT services / outsourced software development to healthcare leaders, over time, we have had to do a lot of proof of concepts, try out various software tools available from various vendors for various customer projects that we have undertaken. We will continue enhancing this guide with more options as we run into them





# Top things to keep in mind during medical software development

1. HIPAA compliance
2. PHI data
3. Storage of patient data (we deal a lot with patient and provider CRMs and had to deal with this)
4. Securing communications (fax, email ,SMS, voice) – we had to deal with this a lot in patient reviews, patient SMS mass texting applications.
5. Push messaging and allowable payloads
6. Transmission of patient data
7. EMR connectivity.
8. Audit trail and history
9. Authentication
10. Authorization
11. Data backup
12. Remediation plan
13. Emergency mode
14. Automatic log off
15. Data encryption and decryption
16. API Gateways
17. Virtual private cloud configurations
18. HIPAA eligible cloud services
19. Patient duplicates
20. Technical prowess of medical business users



# HIPAA compliance – what software developers need to know

You are either developing medical software for your own firm or you are developing one for your client (ie. to be used by others), or provide healthcare IT services to clients.

Either way, your firm (and therefore, by association, you) fall under the supervision of HIPAA.

## Who is a HIPAA-covered entity?

Basically, that's any healthcare provider, any payer/ insurer, any healthcare clearinghouse or a business associate of a HIPAA covered entity.

## Who is a business associate of a HIPAA covered entity?

Generally, a Business Associate is a third-party service provider to a HIPAA Covered Entity who has access to PHI. Any software development firm that is handling any PHI information on behalf of their customer (covered entity) is a BA (business associate). You, as a software developer, would also be classed as a Business Associate if you freelance and are hired by a Covered Entity to develop a HIPAA-compliant app. That too, only when the covered entity (your client) is sharing PHI with you. If your client is NOT sharing any PHI, then you are not covered under the HIPAA rules. Unless you have been asked to sign a business associate agreement, you are not a Business Associate.

This also means that if you develop an app and patients (users) use your app, you are not necessarily handling PHI. If your data was used by a healthcare provider or was used by a health payer (insurance company), then your data is PHI.

If a provider or a payer is asking you to develop software or handle patient data, then your firm has to sign a Business Associate agreement (BAA).

Keep in mind that HIPAA only applies to HIPAA covered entities and their business associates. If your firm has not been contracted by a HIPAA covered entity and is only a business associate, the patient information your application recorded would not be considered PHI under HIPAA.



# What is PHI?

No matter what, you still should know what PHI (Protected Health Information) is and how to store/transmit it. There are 18 identifiers that fall under PHI – make sure you never, ever log or disclose any of those anywhere where it might be stolen, hacked, intercepted etc. Find those 18 identifiers here.

## How to create sample data without actually using PHI?

The 18 identifiers that make health information PHI are:

- 1.Names – very easy to do. Here's a website that allows you to generate random names.
- 2.Dates, except year – generate random DOBs using this.
- 3.Telephone numbers – generate random phones using this.  
Need to verify SMS messages? Use sites like this , this, this or this (many options). Need to receive SMS? Use sites like this.
- 4.Geographic data
- 5.FAX numbers – use the same as above. To receive free faxes, use this.
- 6.Social Security numbers – use this site.
- 7.Email addresses – use this. Want to use temporary email addresses for testing? Use this, this or this (many, many options).
- 8.Medical record numbers – same as random numbers. Use this one.
- 9.Account numbers – same as above.
- 10.Health plan beneficiary numbers – same as above (MRNs)
- 11.Certificate/license numbers – same as above
- 12.Vehicle identifiers and serial numbers including license plates
- 13.Web URLs – use this one
- 14.Device identifiers and serial numbers
- 15.Internet protocol addresses
- 16.Full face photos and comparable images – imgur, <https://placeholder.com/>, <https://picsum.photos/>
- 17.Biometric identifiers (i.e. retinal scan, fingerprints)
- 18.Any unique identifying number or code



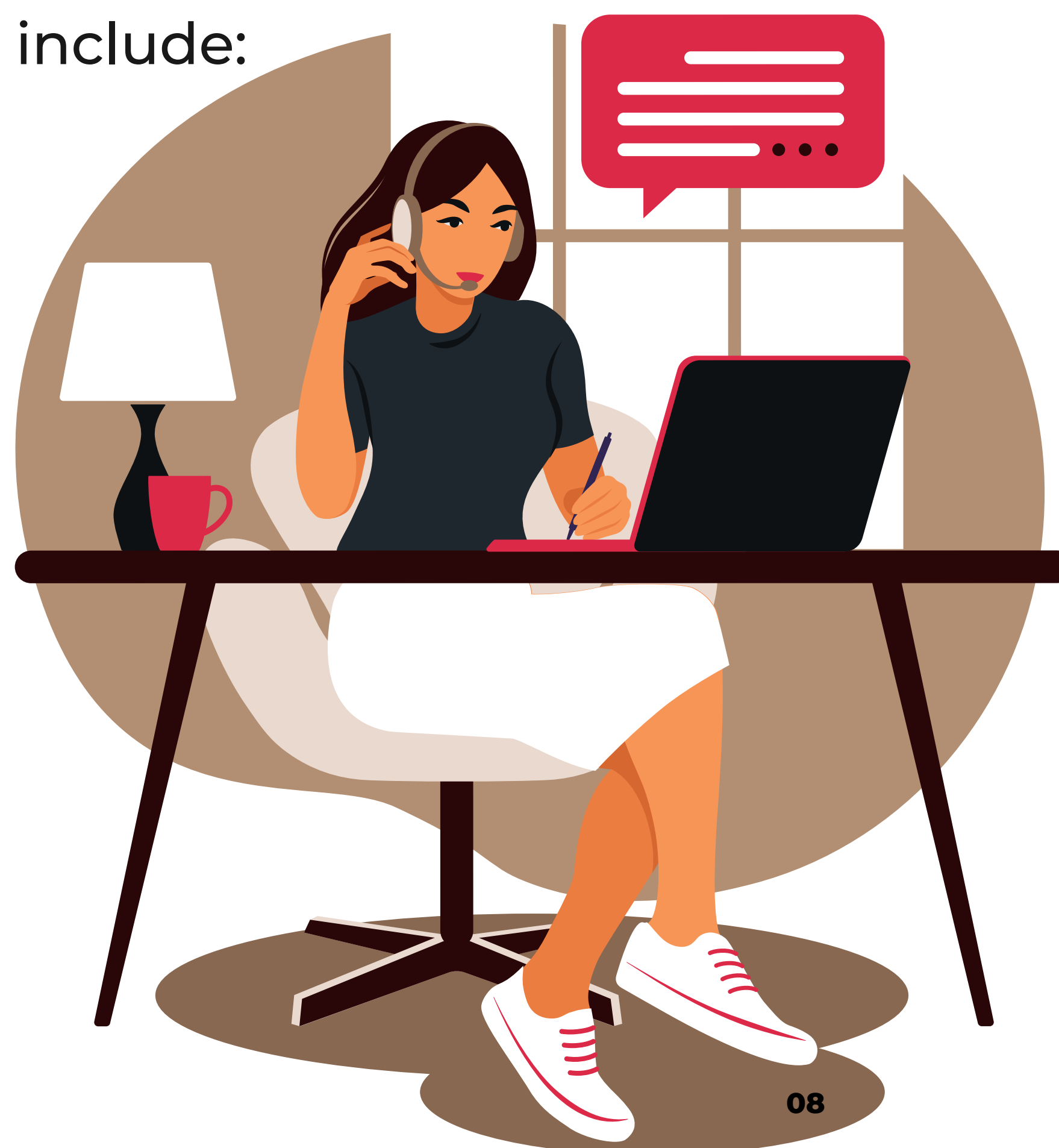
# HIPAA secure messaging options in medical software development

Daily medical practice communications PHI overheads include (not limited to)

- Providers that share various PHI information
- Practice staff that share PHI between each other
- Referring that share PHI with between each other
- Field sales reps or physician liaisons that need PHI information as they go from provider to provider, marketing their practice
- Patients who prefer to text or WhatsApp instead of calling your practice and talking to the practice.
- Vendors faxing PHI
- On top of this, practices have high levels of staff attrition and need to constantly authorize and un-authorize access to PHI.
- Everyone wants instant communication and they expect communications to be as easy as sending an SMS or a WhatsApp. However in healthcare, this is a nightmare as they are directly responsible for protecting patient PHI. The fines are pretty steep.
- Systems that have to integrate over servers (in and outside of the cloud or data centers)
- Systems that need to integrate between various practices (e.g. referrals management)

The various communication channels include:

- Fax
- Email
- SMS
- WhatsApp
- Voice
- Video
- Social media (Facebook, twitter, instagram – however your practice markets itself)







## HIPAA secure faxing

Most of the health systems that still use fax machines are looking to upgrade to leveraging the cloud for faxing. However, most fax servers/vendors do NOT provide HIPAA secure/compliant options. The ones we have worked with already and that we like the APIs of are:

1. Mfax — very good support
2. Aculab — do note that their support is super slow

Other providers include but not limited to are:

1. eFax
2. Srfax
3. Faxage
4. Many, many more



## HIPAA secure SMS

There's no such thing as HIPAA secure SMS. Healthcare practices generally need to communicate a LOT of external parties – e.g. patients, providers, referring partners, physician liaisons in the field (not onsite at locations), payers, pharmacies etc.

Over time, we have noticed that most people are looking to SMS (even more than email). SMS will never be HIPAA compliant – however, with patients, you have the option to get their consent to communicate health information over SMS. If you have that consent right from the first SMS itself, you can transfer your entire conversation with patients to the SMS channel.



## Before you send any PHI, consider these:

- If the patient initiates communication over email or text, according to the FAQs of HHS, you are good to go
- If the patient gives formal consent before any text or email exchange takes place.. Even then you are good to go (as long as you have it well documented/scanned/added to the patient record).
- If you don't have any of the situations above and you want to initiate the SMS communication with the patient, first, send a consent request e.g. "Do you give us the permission to share your health information with you over SMS? As you probably know, SMS is not a very secure channel". If the patient gives you consent – you are still OK to send/receive PHI via SMS.

This approach does not work with pharmacies, referring practices, vendors etc. We have often taken the middle ground. Instead of trying to send PHI over SMS, we still allow SMS communications between parties, however, we only send web links to the patient data being shared.

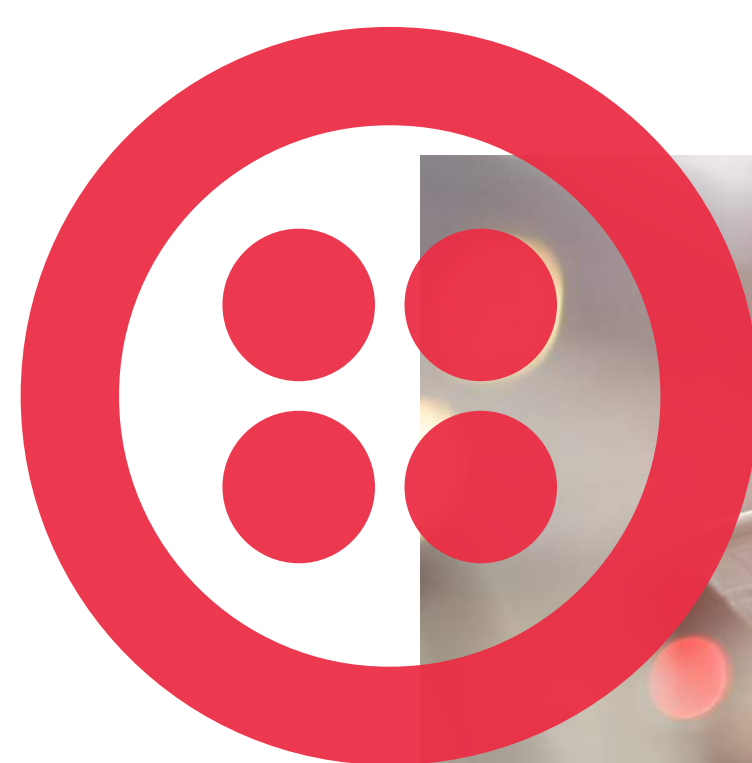
The parties involved and authorized to view that patient data have to confirm their identity, then be authorized to view the PHI. Since communications are going over SMS, in all probability, the link will be opened on the mobile phone itself.

To make it easier for our constituents, we utilize Progressive web applications (PWA) and one time passwords delivered via SMS to identify and authorize users.

We almost always recommend using SMS APIs like those from twilio, bandwidth (better pricing and reliability), Amazon SNS.

Various vendors that offer SMS APIs include (but not limited to):

- 1.Twilio
- 2.Bandwidth
- 3.Plivo
- 4.Telesign
- 5.Nexmo
- 6.Telnyx
- 7.MessageBird
- 8.clickSend
- 9.Many, many more





## HIPAA secure Whatsapp

Again, no such thing as HIPAA secure Whatsapp. We treat Whatsapp just like SMS. For this as well, we end up using Twilio. You can learn more about whatsapp business API here.



## HIPAA secure email

There actually are email options for secure email. However, the challenge is that the receiving party also needs to be using secure email. That's not usually the case and instead it ends up being a very annoying conversation where the email sender sends a HIPAA secure email, the recipient then needs to click on a link in the email to create a password (yet another password to remember), then after reading the email, needs to copy and paste the email to everyone else in the organization that needs access to it (because others in their own organization cannot have access to this secure link that was sent to them). Then, when they need to respond to this email, they cannot just "hit reply" – instead, they have to click on the original link, enter their password, try to upload a file if needed (many such secure email vendors are really bad with attachments), try to CC someone else in that email etc.. This arduous process continues.

We don't blame the software developers for this – we understand why it is needed. To our defense, we try to take the approach where the data remains in a HIPAA compliant/secure application and people that are truly authorized to view that data are sent email/SMS/Whatsapp messages to access the data. If they can verify themselves, they have access to the data. If they want to share the data with someone else, they need to invite that other party to join the network, authenticate and be authorized to view the data.

Our solution is not the best either – but it at least simplifies the convoluted process a little bit more.

For transactional emails, we almost always end up using Sendgrid. However there are many other providers like:

1. Mailgun / mailchimp
2. Constant Contact
3. CampaignMonitor
4. Many, many more.



## Voice options – conduit exception rule

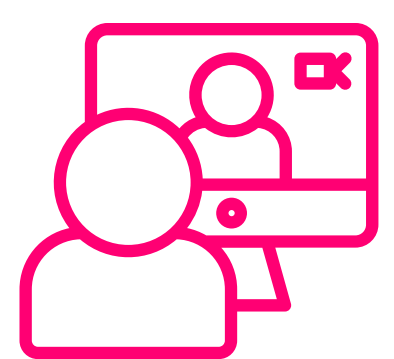
We do a lot of programming for voice that include click to call, Amazon connect contact center voice, automated dialing etc. For most of our customers, we recommend using Twilio or Amazon Connect Contact Center. They will sign BAAs (Twilio started this only recently, as of writing).

What's most important to understand is what you can bypass the BAA due to the Conduit Exception Rule ([link here](#)). It is understandable to think that just based on the nature of software programming, some data *\*will\** be stored, but as long as the vendor guarantees that it is transient data not permanently stored, you are OK with the conduit exception rule.

However, do NOT fall for this.

Vendors often try to classify themselves as conduits – when they truly are not. E.g. email service providers, fax service providers, cloud service providers, and SMS and messaging service providers try to say that they do NOT fall under this rule.

They are NOT and do not fall under the Conduit Exception rule. They need to sign BAAs if you are going to transmit any PHI.



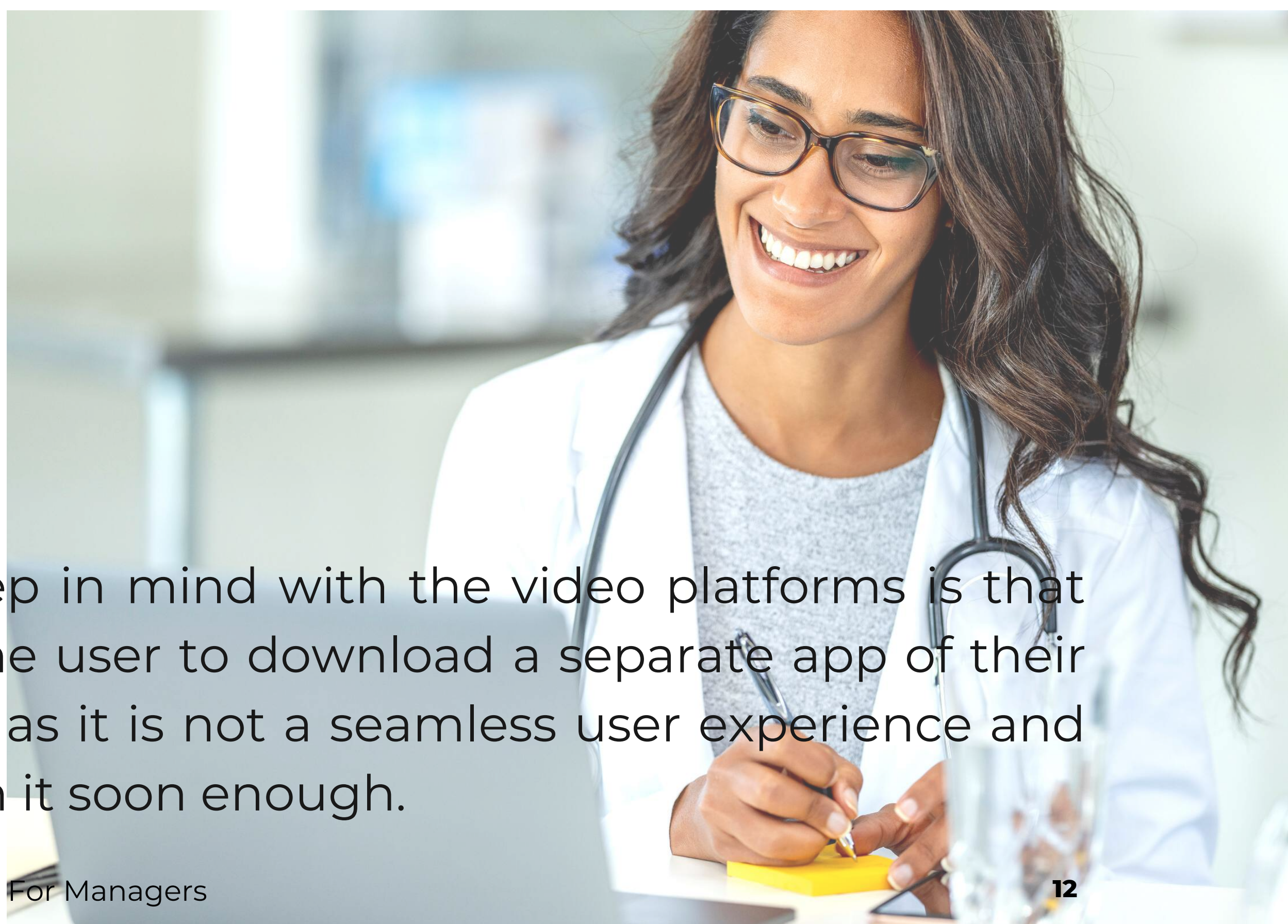
## HIPAA secure Video options

We have only used OpenTok thus far and they do sign BAAs. Hence, we recommend using their APIs. We would never recommend developers to undertake creation and maintenance of video infrastructure. It is exceedingly complicated and you are better off leaving this to the vendors specializing in video infrastructure. STUN, TURN and signaling are not trivial (see link).

There are several vendors in this category including, but not limited to:

- Twilio
- OpenTok
- Mux
- Zoom
- Vidyo
- Sightcall
- Voxeet

What you have to keep in mind with the video platforms is that some of them force the user to download a separate app of their own. Try to avoid that as it is not a seamless user experience and typically folks abandon it soon enough.





# Chatbots to solve your social media and website communications



We knew that sooner or later, we were going to have to consider chat bots. The problem is that these days everyone is always ON and always connected. Our clients' practices get pinged via Facebook and their websites for questions, appointment scheduling/rescheduling/cancellations at all times of the day (yes, even at late nights).

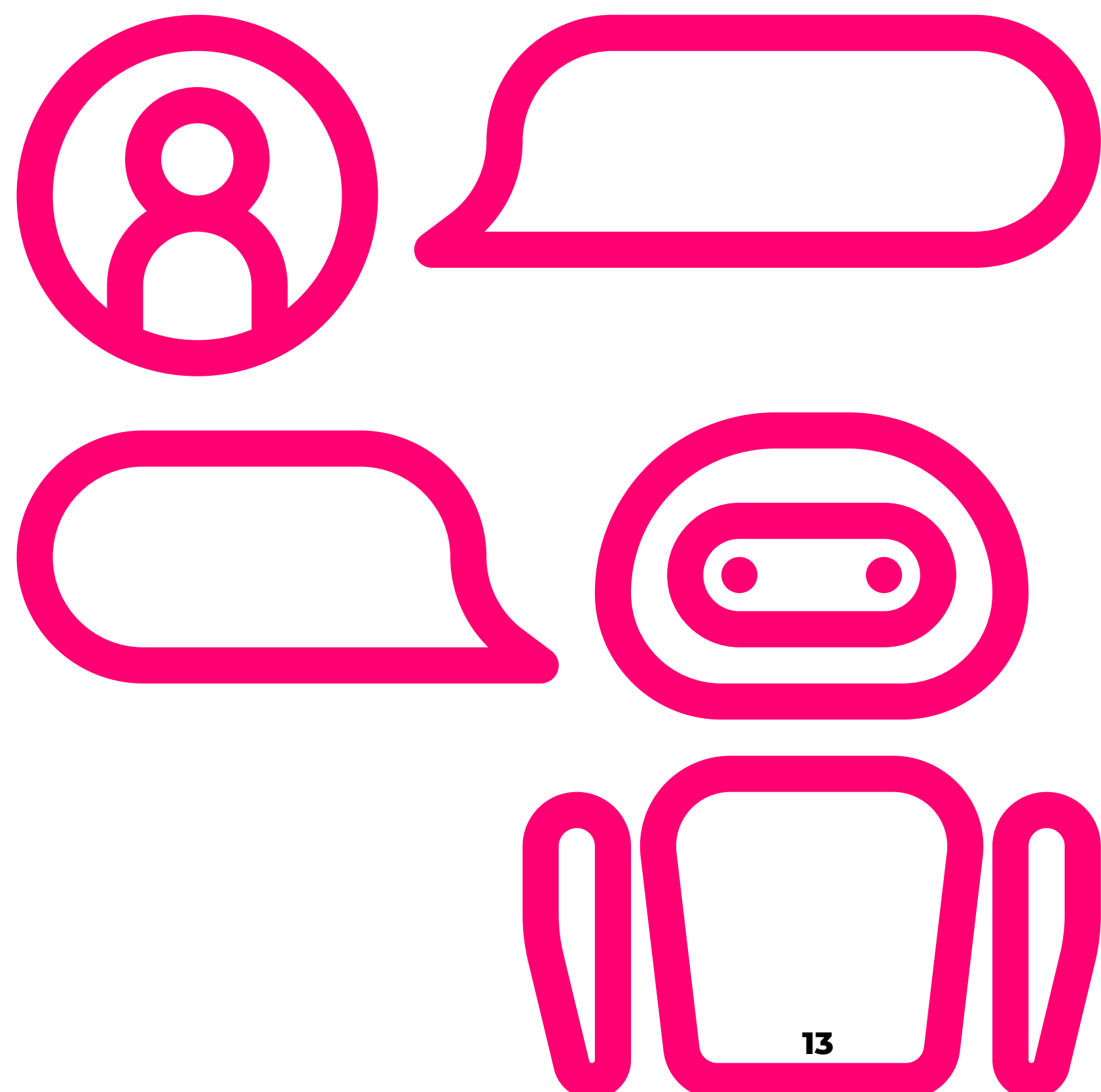
You are never going to have the wherewithal to afford a 24×7 staff. Even if you do, you are not going to be able to solve all problems 24×7. That's where you are going to need to employ chat bots.

In fact, chatbots help you reduce the phone calls to a great extent as well. They are the first line of interaction that our partners and patients face that help them either answer their own queries or be directed to the right person in our clients' practices.

As you already know (and have probably used many chatbots yourself already) chatbots are almost like text based chatting/messaging with the same HIPAA regulations as well. You cannot share any PHI over a chatbot unless the patient consents to it.

There are many vendors that provide chatbot apis, so you don't necessarily have to build anything from scratch.. Take these for example:

- [Getstream](#)
- AWS
- Microsoft
- BMC
- [LivePerson](#)
- [BotKit](#)
- Rasa NLU
- MANY more..





As you start with Chatbots (and if you are really good at mastering this channel to reduce the number of support calls your staff have to handle) you will probably start trying to make your chatbot a bit smarter.. Ones that predict where the conversation is going.. That's where some of these prominent AI Services companies come into play.. I doubt you are going that far.. But if you do get your chatbots to reduce your customer support calls, you probably want to consider the best like

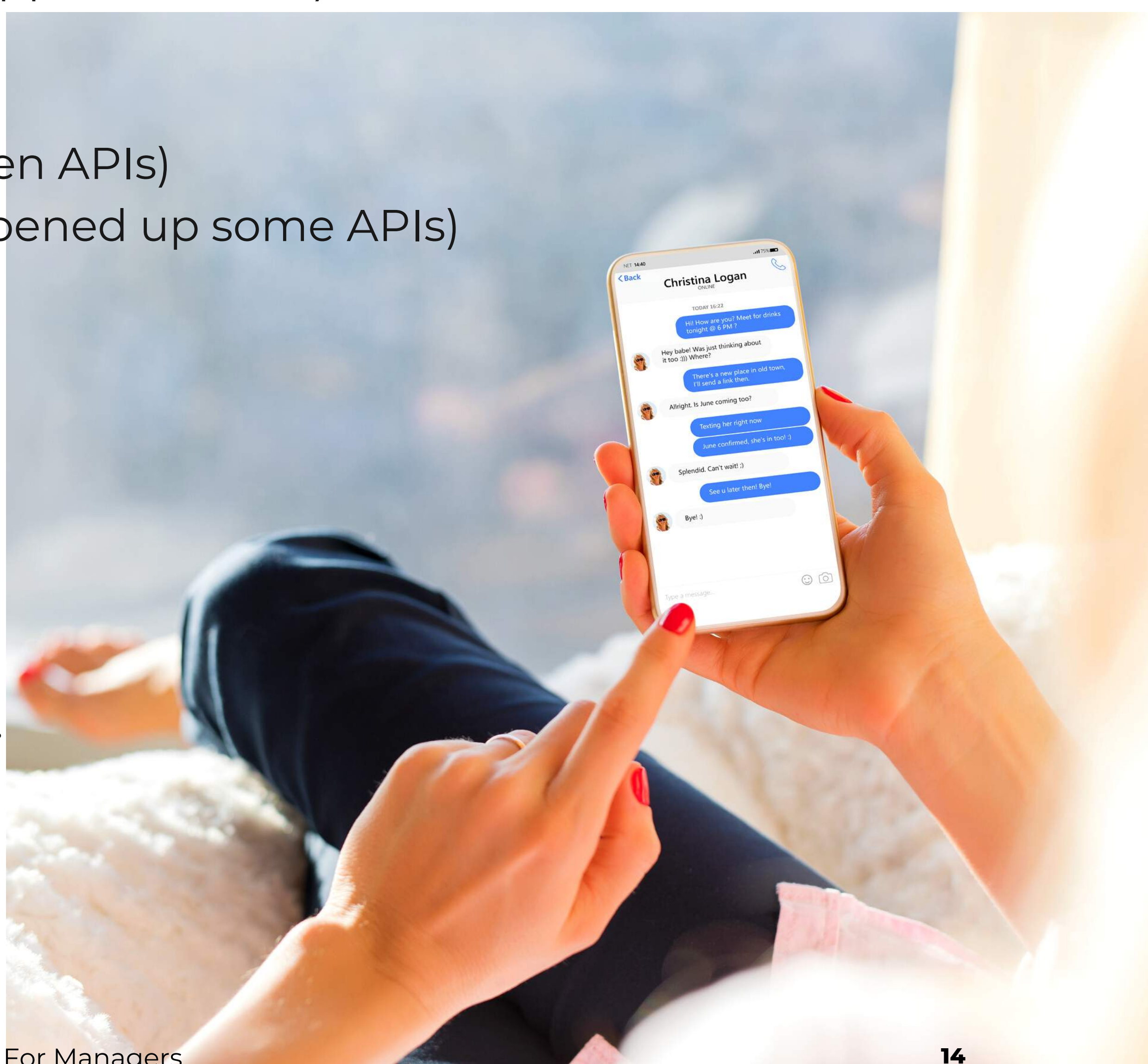
- Wit.ai
- Api.ai / Dialogflow
- LUIS.ai
- IBM Watson

Regardless of what you do, do keep in mind that all these need to be tied into your EMR to really provide value. Without that, it's a bust.

## HIPAA secure real time / chat communications to use for medical software development

There are many vendors who have already solved the really difficult aspects of real-time communications for you and there is absolutely no reason for you to reinvent the wheel. The last time we went through this research we found many vendors that have real time messaging platforms. Here's a partial, non-exhaustive list

1. GetStream (their support is stellar)
2. Pubnub
3. Twilio
4. Telegram (it has open APIs)
5. WhatsApp (it has opened up some APIs)
6. Updox
7. Pusher
8. Cometchat
9. Firebase
10. Solace
11. Informatica
12. Tibco
13. Many, MANY more...





What do you really want to concentrate on are the features that bring more value to your practice, rather than concentrating on the messaging infrastructure itself.

In fact, we would contend that you need to concentrate LEAST on the chat APIs.. that's a problem you should outsource to a vendor that does this for a living... for a price.

We always recommend using Getstream due to their stellar support and the fact that most of their sample applications cut down the amount of coding you have to do. On top of this, they do have the feeds APIs (their origin has been in feeds technology) that greatly help you in case you want to take the route of creating feeds in your application.

## Mobile and web push notifications

We rely on push notifications these days, so whether you have a web or a mobile app, you are going to need real time push notifications. However, keep in mind that to be compliant with HIPAA security guidelines – you CANNOT share any PHI in push notifications without users explicitly consenting to taking FULL ownership of their own PHI and sharing the same via push notifications (e.g. see how Siilo app does it).

Yes, it is that big a deal. We are all used to seeing a preview of our messages on the locked screen via a push notification, but that's not going to fly in a HIPAA secure messaging platform. You need to be super careful about this.

Mobile push notifications have two main vendors anyway – Apple and Google. You can deal with Apple (APNS) and Google (FCM) directly from your platform OR you can offload this headache to vendors that handle push notifications for you. There are several vendors that come to mind including but not limited to:

1. Pusher
2. Pushwoosh
3. OneSignal
4. Amazon SNS
5. Carnival.io.
6. Kumulos
7. Urban Airship
8. Leanplum
9. Intercom.
10. Many, many more..





If you do decide to use a 3rd party vendor (we highly recommend it), make sure that they sign a BAA OR better yet, do NOT share any PHI via push notifications. That way your vendor does NOT have any PHI that it can compromise. Make your push notifications as simple as “You have a new message” or “You have a new referral” or “You have a new reminder”. This way, your application is NOT sharing any PHI with the 3rd party vendor.

## HIPAA security of media being shared and stored

People are going to share PHI – let’s just agree on it. That’s the whole reason why you are reading this guide anyway. Think about this – they are going to share patient records or images or screenshots etc. This is going via the messaging api vendors, and will need to be stored somewhere (in most cases, the cloud).

You have choices – you can store this in the cloud vendors storage offering (e.g. Azure, AWS etc) that are dirt cheap.. Or you can have your messaging vendor store these files for you (of course, HIPAA secure, BAA signed).

Take the easier route – if you have 1 vendor that you can limit your exposure to.. Always choose that. It allows you to hold \*someone\* responsible..one throat to choke.. And not have to get a run around when things go wrong (and things will go wrong).

One thing you do need to keep in mind here is that if you have mobile apps (in all probability you are going to have that), make sure that the PHI media being shared via your apps does not go into the camera roll.. Rather, is stored in a special, locked and encrypted folder on your users’ phones.





# Authentication and authorization of people using your platform



Hopefully your practice/customer uses google business apps or microsoft outlook or some kind of authentication mechanism. We have come across many healthcare practices where not all their staff actually use the company email.. Instead, many of them are not given individual emails.

However, the one thing that does remain is that everyone on your staff will have their mobile phones.

To make things easier, you have a couple of options:

- Authenticate people using their work emails. In this case, you are going to need a single sign on mechanism so that your users just need to use their Google/Microsoft emails to sign in once and then use your application
- Authenticate people using their mobile phones. In this case, you are not going to have the single sign on headache
- Authenticate people using a typical sign up / login / reset password kind of mechanism

Finally, you can always make your platform as an invite only one. This at least takes care of one headache for you – spammy and fake users!

Now that you have authenticated your users, let's talk about authorization.

Of course, there are several staff in your practice that need access to ALL of your EMR data so they should be authorized to access your EMR data and tie it into their usage of the communications platform.

But how about the rest of the users? Sure, they are authenticated and can use your platform, but are they authorized to take all actions on the platform? Are they allowed to access all patient records? Are they allowed to add other users to your practice's communications platform?

Think through authentication and authorization very well..



Does everyone in your practice need access to patient data? Even for doctors – do they need access to records of patients that are not theirs?

You already know that your patients need access to only their own patient records, so they should not be authorized to access anything but their own medical records.

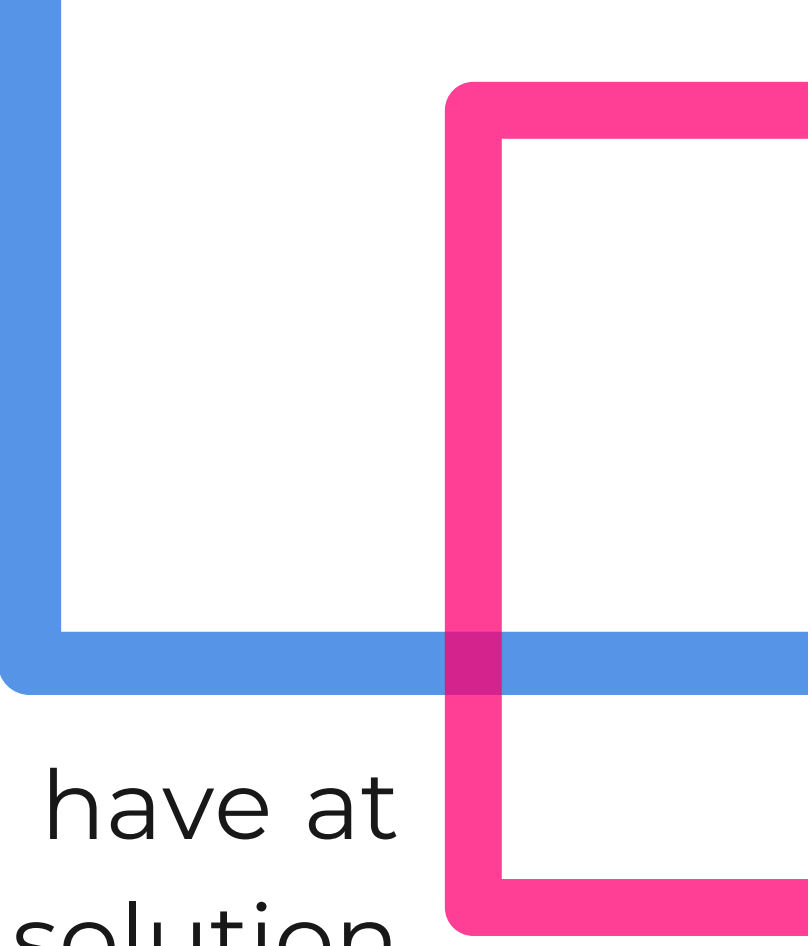
How about your partners? You know very well that while they have shared access to common patients, they should not be authorized to access the rest of the data in your EMR.

You don't actually have to create authentication and authorization mechanisms for this platform yourself as there are several options here as well (listed below). One thing to keep in mind here is that the more moving parts you include in your solution, the more headaches it does introduce.. But at the same time, these authentication and authorization platforms do a lot of the heavy lifting for you.

E.g. These platforms take care of:

1. Personalization
2. Passwordless registration
3. Scaling up to meet higher demand/traffic
4. Consistency in users' experience
5. Social profile enhancement
6. User analytics
7. Centralized management
8. Multiple device management
9. Unusual sign in attempts
10. Security and compliance
11. Multi factor authentication
12. Device based policy control
13. Attribute based policy control
14. Many, many more headaches





Weigh your options based on the developer strength you have at this moment and also the total cost of ownership of your solution moving forward. You don't want to have to deal with headaches just for your users to be able to sign in, sign up etc

There are some great options for vendors that will handle this for you

1. [AWS Cognito](#)
2. [Auth0](#)
3. [Microsoft](#)
4. [Google](#)
5. [Okta](#)
6. [Ping identity](#)
7. Many, many more

Do keep in mind that having a 3rd party vendor manage your authentication and authorization is not as easy as it sounds. You have to ensure that data is replicated to your internal systems as well. Who is going to be the system of record? Your internal system or the 3rd party vendor? How are existing users going to be migrated to the 3rd party vendor? Who maintains the passwords? Do systems that are entirely internal also have to use the 3rd party APIs?

Weigh in all the pros and cons before making this decision.

# Ability to integrate your EMR/EPM with the messaging platform

Find a primer for EMR integration [here](#). EMR integration of your software (if you are a third party vendor) is not something you can rely on – it takes a while to get EMR integration done (not for technical reasons, but for other health IT projects almost always take priority before a 3rd party's EMR integration).



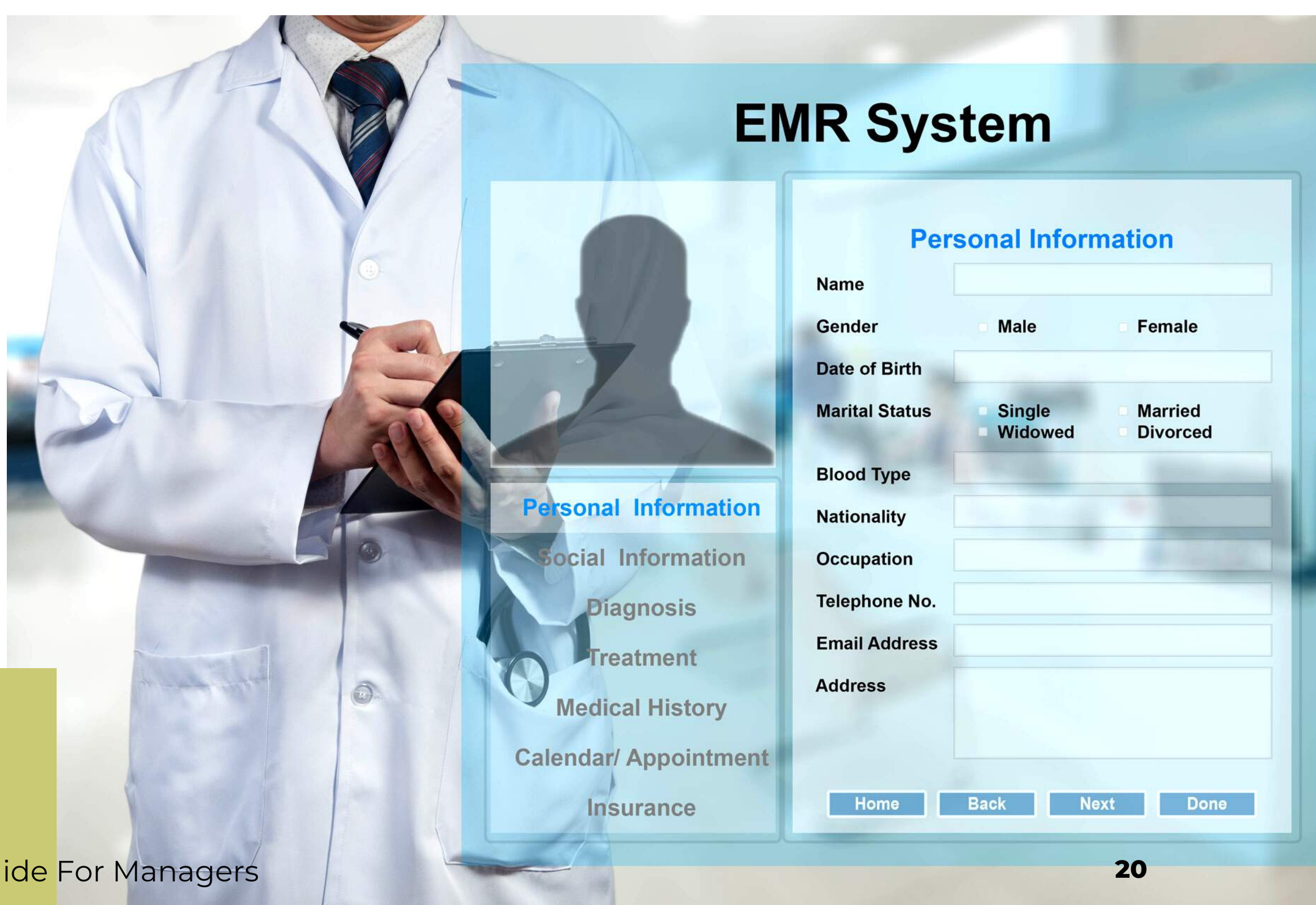
Keep in mind that there are various kinds of staff. Try to understand their daily workflows to develop your software accordingly:

- Staff that are always seeing patients, moving from room to room.. And are always near the EMR
- Staff that are involved in practice management operations – not necessarily always in front of the EMR but are mobile within the practice
- Staff that are in marketing, out on the field and almost never near the EMR
- Staff that are dealing with practice management, not mobile, always having access to the EMR BUT are not on the EMR for their daily jobs (e.g. insurance verification, calling patients etc)
- Staff that were on their mobile phones had the most demands – they could not open up EMRs from their phones and even if they did, they needed to be able to move information from one app to another.

In our experience, staff that were not mobile didn't always have the EMR open nor did they have any communications platform always open – but they needed to be notified in real time for questions and needed to be able to respond with PHI information immediately.

Tie in your EPM/EMR to the messaging platform and your software application ASAP – you will see a much higher adoption of your platform and will recoup your investment multi-fold.

The challenge really occurs when you have to communicate between various EMRs across practices and even within your own health system if you have multiple EMRs.





# HIPAA secure hosting and EMR integration



You don't have to necessarily build it all out yourself as there are some rock solid vendors that do this for you. In the end, this really involves

- Building your EMR integration / interfaces (HL7 or otherwise)
- Standing up your EMR integration infrastructure in an HIPAA secure/compliant environment

A few respectable vendors that handle EMR integration in the cloud include

- Datica
- RedoxEngine
- Corepoint
- Mulesoft
- Iguana
- Sansoro
- Apigee

However, do keep in mind that no matter what you do, you are going to have to ensure that your integration infrastructure is HIPAA secure.

So, if you are taking the route of your messaging vendor being in one place, your authentication vendor being in another, your integration being in yet another place. Think this through well.

Folks like Datica, Aptible give you a slam dunk easy way to manage your healthcare applications in a HIPAA secure environment. You could argue that AWS, Azure does this as well (more on this later) but these cloud vendors only give you a **HIPAA eligible** environment. Compliance is actually YOUR headache.. Not theirs – because they espouse the shared responsibility model.

The beautiful thing about Datica and RedoxEngine is that they both run their integrations on the well tested MIRTH engine.. But they handle the integration infrastructure for you as well – in addition to managing the interfaces for you. And if you have to pass compliance audits.. Well, guess what ? That painful process is better outsourced to Aptible, Datica etc, rather than to be taken on by your staff .. you don't want to hire full time compliance staff do you?







# MEDICAL SOFTWARE DEVELOPMENT – GUIDE FOR MANAGERS

---

Written by Nisos Health ([nisos.health](https://www.nisos.health))

## **Want to get started?**

Our software and services help providers reduce operational expenses, increase collections, improve patient outreach and patient experience. Healthcare organizations rely on us for call center solutions, healthcare software services, healthcare BPO, medical billing, revenue cycle management solutions.



Thank  
you!



**USA:** 134 N 4th St, 2nd Flr,  
Brooklyn, NY 11249.

Tel : +1-844-900-2523

Fax: +1-855-453-7846



**India:** 201/202, Lakhani  
Centrium, Sector 15, Navi  
Mumbai, 400614.

Tel : 22-4127-0688



Nisos Health



<https://nisos.health>



1-844-900-2523



[hello@nisos.health](mailto:hello@nisos.health)