TRILLIAN

The ultimate guide to HIPAA-compliant IM for patient success in healthcare

CONTENTS

Introduction

Instant messaging (IM) software has revolutionized the way that people communicate in the workplace. And of course we would say that, wouldn't we? Still, you don't have to take it from us: according to a report from The Radicati Group, the number of instant messaging accounts has grown from 3.2 billion to 3.8 billion over the last four years. In business, it's 'growing at a much faster pace than the use of IM by consumers.'

So yes, instant messaging is a more efficient way to communicate when compared to traditional methods like email and calling. But, here's the problem: **users aren't as bullish about security measures**. A Reportlinker survey found that 57 percent of users felt they couldn't be sure that chat data was entirely private.

That may not be a huge problem if you work in an unregulated industry. If you're in healthcare, however, data security is vital for success – it's the difference between compliance and massive fines.

HIPAA compliance

If you're reading this, it's safe to assume you know what HIPAA is. For those that need a refresher, **HIPAA stands for the Health Insurance Portability and Accountability Act, or in layman's terms, the law that ensures private health information stays private.** It's one of the cornerstones of a successful healthcare practice.

Noncompliance fines are tiered according the level of culpability, but violators can expect penalties of anywhere from $117 to $58,490 per infraction, with an eye-watering maximum annual penalty of $1,754,698 (as of 2019). In short, jeopardizing patient privacy is taken extremely seriously.

HIPAA-compliant instant messaging presents a potential communications and efficiency boost that can significantly improve patient care. But how can the financially terrifying risks of noncompliance be safely navigated to improve patient experience? Well, knowing the risks is the first step towards successfully – and safely – adopting IM technology in your healthcare organization.

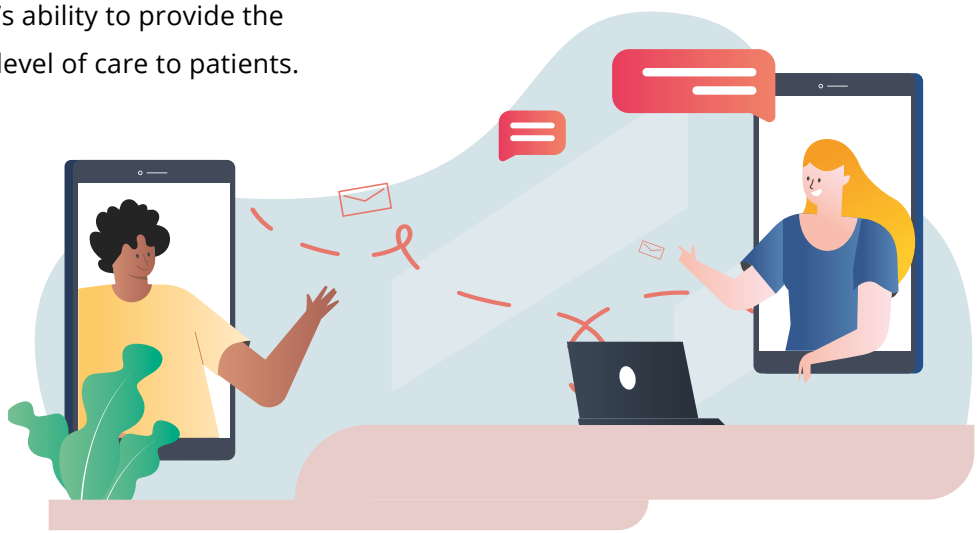
Threats to customer success

The penalties for noncompliance are suitably scary, so it's worth knowing where things can go wrong with unsecure IM. Doing so will make it possible to plug those gaps before they cause problems.

Here are the most significant threats to patient and customer success presented by improperly adopted IM:

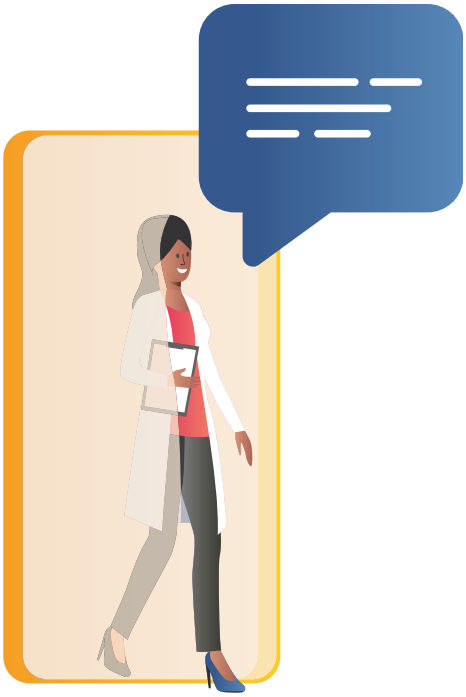
Noncompliance penalties
As mentioned above, failing to comply with HIPAA regulations translates into hefty fines. Those fines, if severe enough, can have a knock-on effect on your organization's ability to provide the appropriate level of care to patients.

Unregulated messaging
Protected health information (PHI) should, as the name suggests, be protected as much as is reasonably possible under HIPAA guidelines. The wrong IM software can undermine this in many ways, from **mobile lock-screen notifications that can be seen by all, to automatic cloud backups of files and unencrypted messaging.**



Lack of policy

A 2017 study found that while over half of clinicians use text messaging on the job, only a quarter reported that their organization was using a standardized, secure messaging platform. A detailed messaging policy is essential, especially if employees are using their own devices that could be lost or stolen, which may compromise patient data. Failing to do so can lead to the kinds of results seen in the UK, where 200 NHS trusts failed a government security audit in 2018. This resulted in a £21 million investment to improve cybersecurity.



Loss of trust

The trust your patients have in your service is on the line, and they're skeptical about electronic communication as it is. The Office of the National Coordinator for Health IT found that a massive 66 percent of people have reservations about privacy when health information is electronically exchanged.

Research has also shown that there is a direct correlation between patient-clinician trust and positive health outcomes, as well as patient satisfaction. These factors lead to a boosted bottom line for health providers – a 2018 publication from the National Academies of Sciences, Engineering and Medicine offers a neat summary: **'Research has shown that hospitals with more satisfied patients make more money.'**

The benefits of IM

There are several reasons that the healthcare community is beginning to rapidly adopt IM. Whether you're making the case for IM to higher-ups, or you're weighing up the decision yourself, here's why it's an essential tool for healthcare organizations:

Streamlined communication

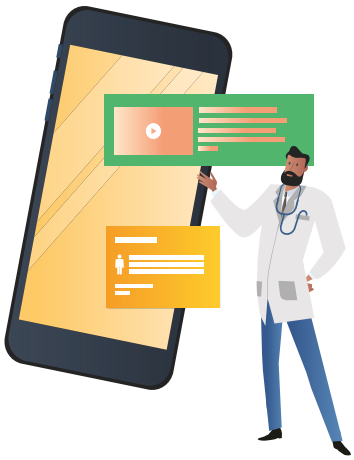
It's no surprise that IM is a good deal faster than email – 'instant' is in the name, after all. Instant messaging allows for the quick transfer of Electronic Health Records (EHR) between departments that would otherwise take longer to complete. This, in turn, cuts response times down, which is always good news for patient experience.

A 2017 study of WhatsApp use by clinicians bears this out, concluding that instant messaging has 'the potential of facilitating clinical communications, enhancing learning and improving patient care'.

More efficient processes

IM has the potential to replace traditional paging systems and lines of communication for a huge number of tasks, especially when used on smartphones. The processes in a healthcare organization can, as a result, eliminate time or location-based communication delays while people are on the job.

A 2016 study of four hospitals using secure IM concluded that 'a mobile application can improve communication and workflow efficiency among providers in a hospital.' Better processes mean happier, more adequately served patients.



A HIPAA-compliant IM checklist

We've established that IM is a potentially valuable means of communication to add to your existing technology stack. We've also established that there are significant risks if it's not properly implemented. This checklist will help you ensure that you've got everything you need in a secure IM platform:

Essential HIPAA requirements

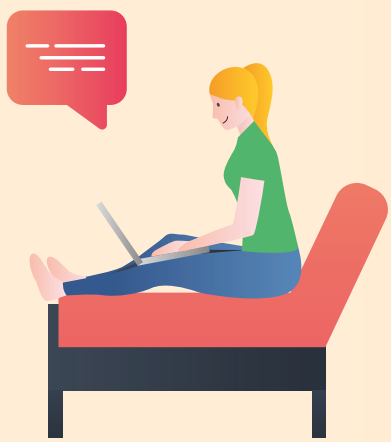
Perform an IT risk assessment: Whether you're adopting new technology or not, it's worth assessing the risks to PHI that your current digital tools present. You'll want to then create a dedicated risk management policy in order to remain HIPAA compliant.

Create an IT policy: There should be a policy in place for the use of mobile devices and computers. That way, everyone in your organization knows exactly how they're expected to transfer information safely.

Prepare for an emergency: Part of your policy should include a plan of action in the event of an emergency, digital or otherwise, that will protect data.

Implement secure access: Any access to IM software must be restricted with unique passcodes or PINs for each user, especially if employees will be bringing their own devices to work.

Record all activity: Ensure that your IM software allows you to record and archive a log of all the activities and messages that take place. This is especially important in the event of an audit, and for flagging inappropriate use before it can snowball into a bigger problem.



Essential IM requirements

Personalized security: Every organization is different. It's important to choose an IM platform that allows you to customize things like data retention, identity and access management, cloud back-ups, and file-sharing, to suit your business' needs.

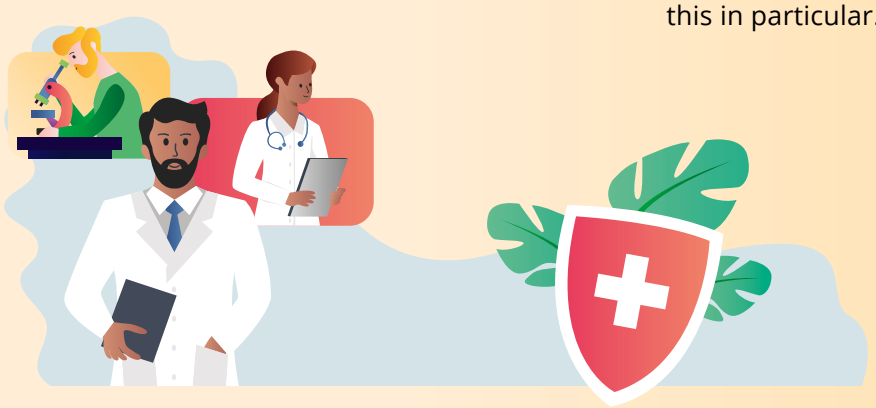
On-prem hosting: For even more compliance peace-of-mind, look for a solution that allows you to host the service on your own servers. It'll mean you don't have to worry about data breaches that are the result of negligence on the part of cloud providers, and it affords you further tailoring of security measures.

Certification: IM providers can say that they're secure, but without certification this doesn't mean all that much. Look for accredited software whenever claims are made about regulation compliance.

Remote control: Any software that involves the transfer of PHI should make it possible for data to be wiped remotely in the event of a breach.

Integrations: IM can further improve workflows (and the patient experience as a result) if it's able to integrate with technology you're currently using. If PHI can be pulled directly from your electronic health record system, for example, you'll be cutting another step out of the equation and maximizing efficiency.

Cross-device use: Any messaging software you use should be securely accessible on both computers and mobile devices, whether they're provided by the organization or you have a BYOD policy.



Individual and group chat: When a team of clinicians is working with the same patient, it can be helpful for several people to share information in a group chat. Make sure the software you're choosing allows you to do this, as well as control who accesses which chats.

Urgent alerts: Important, time-sensitive information abounds in the healthcare industry. Your IM software should facilitate different levels of urgency when it comes to notifications. That way, staff know what needs their immediate attention and what doesn't.

Encrypted messaging: Messaging should be encrypted to a suitable level and shouldn't provide the ability for external parties to gain access to your data. Mainstream, ad-supported consumer platforms struggle with this in particular.

Say hello to Trillian!

At Cerulean Studios, we provide Trillian, an instant messaging platform that prioritizes security and ease-of-use. We've spent the time to achieve HITRUST CSF certification because securing and safeguarding customer data is an important part of our business model. Data is encrypted in transit and at rest, customizable file retention means that data can be wiped after a specified period of time, and we're one of the few IM providers still dedicated to providing an on-prem hosting option. In short, we give you as much control as you want over your data and internal messaging policies.

If you'd like to learn more about Trillian or talk to us about your organization's requirements, feel free to contact us here - we'd love to chat! Interested in giving Trillian a go? You'll find links for a free trial and a demo on our website.