#### Encryption Security vs. usability

From a technical standpoint, it makes sense to encrypt every message that goes out to your clients, but because of the wide variety of ways your clients use email, it may not be very easy for them to actually open and read your messages.

Traditional email encryption tools require that both parties mail servers be setup with the same protocols, which just isn’t practical unless you have a small number of clients that are somewhat tech savvy.

[Generating and distributing your own encryption keys is another option](https://blog.encyro.com/best-email-encryption-services/), but that often means that your clients need to download and install specific software or sign up for an account on the platform you choose to use.

Many businesses have created client portals on secured servers to interact with their clients, but forcing clients to login to a separate website every time you want to communicate with them isn’t really all that convenient for your clients either.

#### Webmail options

Many popular webmail services such as Gmail automatically incorporate TLS or Transport Layer Security (HTTPS) whenever their users are signed into their accounts.

This ensures that user messages are encrypted between their computers and Google’s mail servers to prevent others from easily reading the contents. If you use Gmail and your recipients are also using Gmail, your interactions are automatically secured all the way through.

If you use Gmail and your recipient uses another service that does not support TLS, Google has to convert the message back to an unsecured format before it’s sent to your client’s mail server.

If asking your clients to create an account on the same TLS supported-webmail service is practical, that’s one approach, but it may be better for you to determine if what they are already using supports TLS.

An easy way to do this is by using the [LuxSci TLS Checker Tool](https://luxsci.com/smtp-tls-checker) to check the domains for your clients for SMTP TLS support.

Keep in mind, using TLS does not prevent either of the mail servers from being able to see what is in your messages, so if that level of security is a requirement, you’ll have to use one of the more technical methods of encryption.

#### Alternative messaging options

Many of today’s popular messaging platforms such as Skype, WhatsApp, Signal, Facebook Messenger and Apple’s iMessage incorporate end-to-end encryption, which will keep your communications private.

Some only allow messages, while others like WhatsApp allow you to send attachments, so if your clients are already using these platforms, it’s another way to avoid the potential confusion of a complicated email encryption system.

# **What Type of Email Encryption is Right for Your Organization? — Security Boulevard**

[**LSC Network**](https://lscnetwork.blog/author/netzer9/) / [2 weeks ago](https://lscnetwork.blog/2020/06/22/what-type-of-email-encryption-is-right-for-your-organization-security-boulevard/)



Language English Tags: Encryption Email Security eDRM For all the growth in use of productivity tools such as Trello or Slack, for all the deployment of collaboration and file-sharing systems such as Dropbox and Huddle, email remains the most widely-used business communication tool, by a significant margin. The Radicati Group has predicted that the number of worldwide email users will grow to more than 4 billion at some point during 2020, while the total number of business and consumer emails sent and received will exceed 306 billion by the end of 2020. By the end of 2024, this will have grown to more than 361 billion.

Email – A Gateway for Potential Cyber-attacks The sheer volume of emails being sent means that email is also potentially one of the biggest areas of cybersecurity vulnerability for any enterprise. To help address this, the National Cyber Security Centre recommends that data in transit networks are given adequate cybersecurity protection and that emails are encrypted to prevent them being read by anyone other than the intended recipient. Encrypting emails renders the content unreadable as they travel from origin to destination, therefore providing an additional layer of security and protecting the data in transit from would be cyber-attackers or in scenarios where an employee accidentally sends confidential information to the wrong person. Encrypting emails is also considered best practice in many industries, especially those that are required to comply with strict regulations and protect Personal Identifiable Information (PII) and Personal Credit Card Information (PCI) data. Many cybersecurity vendors offer encryption options with their Secure Email Gateway products, but there are many different email encryption options available. To help determine what type of email encryption is right for your organization, here’s a look at some of the most popular: Transport Layer Security Encryption (TLS) This is the most simple of email encryption types but it is highly effective for organizations that only require encryption on messages between it and other organizations.

TLS connections can be ‘opportunistic’, allowing encrypted messages sent in this mode to automatically seek out and favor a connection using TLS. It can also be used when connections between organizations are mandated and have pre-specified encryption strengths.

Used in this way, TLS ensures that messages are only sent if the appropriate level of security is achieved. Message Encryption (S/MIME and PGP) Any leading encryption solution will support international standards for the OpenPGP and S/MIME message formats. These allow communications between recipients who use standard email clients. Sophisticated email gateways can also use these to create policy-based secure connections between gateways or from gateways to recipients.

Depending on when the message is encrypted, i.e. at the desktop or at the gateway, content filtering engines can still ensure that communications adhere fully to corporate email policy, or blocked if the system is unable to decrypt the message as it does not have a suitable decryption key to open it. Best Efforts Encryption Not all recipients will use OpenPGP or S/MINE, so when configuring encryption policies, it makes sense for the gateway to try and find the next strongest alternative and use that rather than not deliver the message at all. Commonly this is password protected PDFs or Zip files.

Password protected PDF files are a popular format for secure statement or document delivery. Web Portal-based Encryption The levels of technical understanding of an intended recipient can dictate which method of encryption is used. Portal-based encryption is an easy-to-use method that requires no knowledge of encryption. Encrypted email messages are sent using an encryption portal which can then be opened on any type of device using a standard web browser without the need for plugins. When this method is invoked the user receives an email to say that they have received an encrypted message through the portal and they simply browse to it, authenticate the message, and read it. Portal-based encryption can be a cloud service, or it can be provided ‘on-premise’, where the system can be completely under the organization’s control. Information Rights Managed (IRM) Like encryption, IRM (also known as enterprise Digital Rights Management (eDRM)) secures the message and file in transit, but unlike encryption, it retains access control even when the recipient has received it in their inbox.

IRM allows senders to set a read by date for the message and attachments or retract access whenever they choose. IRM can also prevent the recipient from sharing the data with other parties by preventing screen prints, message forwarding, and watermarking the files. Clearswift Encryption Options Clearswift has built a reputation as a provider of some of the world’s most effective email encryption solutions.

The Secure Email Gateway provides TLS encryption as standard and S/MIME and PGP encryption as a cost option. Additionally, we work with some of the very best technology partners to provide our customers with a complete range of additional encryption options, including: CipherMail – on-premise encryption portal Cryoserver – secure email archiving Echoworx – hosted encryption portal Seclore – enterprise Digital Rights Management To learn more about Clearswift’s email encryption solutions, ask us for a demo. Ask us for a demo Related resources: Encryption Options in the Clearswift Secure Email Gateway Six Step Guide to Email Security Best Practice On Demand Webinar: Improving Data Loss Prevention and Encryption Controls to Maximise Email Security Blog: Moving on From Encryption – the Case for eDRM Tags: Featured: 1

I was trying to read all the message(email) documents of the user pro-grammatically, while reading a document how can i know whether the mail is encrypted/signed?. I can see Encrypt,$EncryptionStatus, EncryptionFlags,Sign properties in message document property. According to the security options in the following image,



How these (Encrypt,$EncryptionStatus, EncryptionFlags,Sign or anyother properties ) property value will change at sender and receiver side?

I am googling for message document properties I am not able to find documents, which has all the message document properties and explaining each of the properties and corresponding value. I was trying to read the documents using c# interop.domino.dll.

# **Advanced Encryption Options**

One of the main barriers standing in the way of email encryption has been the difficulty using encryption services and the lack of advanced encryption options. Trustifi revolutionized email encryption through the integration of advanced encryption options that are easy-to-use and hassle-free to receive and open. The suite of features our robust email encryption platform gives users the flexibility to use their encryption service in ways they may not have imagined.

## The Trustifi Difference

With Trustifi’s encryption software, there’s no worry about an email sitting around in someone’s inbox waiting to be opened or staying available for malicious actors. With the rise in data thefts, malicious actors are increasingly penetrating email platforms with the intention of gaining access to sensitive information. Trustifi addresses this concern by providing the sender with a comprehensive set of tools that gives them an unprecedented level of control over the content that they are sending.

With Trustifi senders can:

* Recall, block, or modify emails that have already been sent or delivered.
* Set expirations for emails so that they aren’t sitting around in someone else’s inbox.
* Prevent printing and remove metadata from attachments
* Add customizable corporate logo and branding to delivered encrypted email.

These features give users end-to-end control over where content goes and how long it lasts at its destination.

## Core Benefits

Trustifi doesn’t just enhance the security of sent emails by allowing you to encrypt it one way, it also provides security features for recipients, too. Given the wide breadth of cybersecurity threats facing modern organizations, Trustifi’s intelligent email security features offer a welcome defense against email-based threat vectors.

Trustifi also augments cybersecurity efforts by automatically incorporating threat detection into inbound emails. With Trustifi, all emails delivered to a user’s inbox are given an authentication score and emails that appear suspicious will be flagged so the user is alerted not to open. No longer will malicious actors be able to simply spoof their email address to bypass company security protocols.

With Trustifi, users know immediately whether an email is verified from an authorized sender or a spoofing attack filled with malware links or bad attachments in an effort to phish financial data.

## Industries

While everyone can benefit from greater security, for individuals and organizations in industries that interact with sensitive data on a regular basis ensuring the security of their data is a primary concern. These include:

* Pharmaceutical and Healthcare
* Financial
* Legal
* Real Estate and Mortgage Brokers

Trustifi’s advanced encryption options make it the ideal email encryption platform for industries that interact with sensitive data, such as personally identifiable information (PII), electronically protected health information (e-PHI), cardholder data, and sensitive personal information.

## Why It Matters

The consequences of a data breach have never been greater. The risk of suffering a breach is growing every day, which is why it's imperative that your email's data is encrypted properly. Even the best cybersecurity implementations efforts to minimize the risk of unauthorized access to data.

Trustifi’s advanced encryption options build on your existing cybersecurity efforts by giving you an additional layer of security. Features such as Inbound Notifications serve as an added line of defense against the ever-present risk of spear phishing.

Effective cybersecurity requires an always-on level of readiness. With Trustifi, you can be sure that every email you send is encrypted and secure, and that every email you receive has been vetted.

# HIPAA Email Encryption: We Reviewed 7 Services and Found the Best

* [January 7, 2020](https://adeliarisk.com/2020/01/07/)
* , 3:28 pm
* , [HIPAA](https://adeliarisk.com/category/hipaa/), [HIPAA and Email](https://adeliarisk.com/category/hipaa/email/)

Trying to figure out the best way to handle HIPAA Email encryption?  How do you send PHI via email and still follow HIPAA?  And how do you send encrypted email in cloud services like [Gmail](https://adeliarisk.com/hipaa-services/#gsuite) or [Office365](https://adeliarisk.com/hipaa-services/#office365)?  These are two of the most common questions we get. It’s an understandable question. Email has become the communication tool of choice in the digital age.

Most workplaces rely on it heavily. If you’re a HIPAA-regulated business, email use gets a lot more complicated. It’s even more complicated when you want to email PHI, or Protected Health Information. Good news: it **is** possible to send PHI via HIPAA compliant email encryption, and we’re going to tell you exactly what it takes! But before we jump right in, let’s review the basics.

## **Table of Contents**

* [Table of Contents](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-0)
* [What is PHI?](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-1)
* [What is HIPAA Email Encryption?](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-2)
* [What is HIPAA Email Encryption?](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-3)
* [Fine, I’m drinking my Ovaltine, but why does all this matter?](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-4)
* [So how do you send secure email?](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-5)
* [1) Get consent to email PHI](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-6)
* [2) The free options (don’t bother)](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-7)
* [3) The heaviest-advertised option: Virtru](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-8)
* [4) The option from your IT company](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-9)
* [5) A clunky option for Microsoft fans: Office 365](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-10)
* [6) Not safe for HIPAA? – SendSafely](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-11)
* [7) The easiest, best HIPAA Email Encryption](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-12)
* [Conclusion](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-13)
* [Get a Free Paubox Trial](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-14)
* [Talk to us!](https://adeliarisk.com/hipaa-compliant-email-7-best-ways-email-phi/#elementor-toc__heading-anchor-15)

## **What is PHI?**

PHI stands for “Protected Health Information.”

PHI is anything that can identify an individual and provide information about their healthcare.

Think of it this way. If you’re emailing ANYTHING that someone can use to figure out medical information, it’s PHI.

For healthcare providers and business associates, PHI is everywhere. Even in places that you wouldn’t think to look, like notes on a calendar or files in a “Downloads” folder. [This infographic](http://blog.securitymetrics.com/2015/08/phi-is-everywhere.html) does an awesome job demonstrating all of the different places where PHI can hide.



<img src="https://adeliarisk.com/wp-content/uploads/2016/08/unsecured-phi-locations.png" alt="hipaa compliant email-unsecured-phi-locations" width="700" height="400" />
Hint: there are a lot of them.

## **What is HIPAA Email Encryption?**

So, you get it: PHI is important. PHI is everywhere. So what do you do?

First, you need to understand the basics of encryption.

Encryption is at the heart of many of today’s data protection tools. It’s an effective way to shield data from prying eyes.

It’s not important to understand how encryption works.

All you need to know is that you start with an ultra-important secret message:

Be sure to drink your Ovaltine.

When it gets emailed out, it looks like this to anyone who tries to intercept it:

—–BEGIN PGP MESSAGE—–
Version: BCPG C# v1.6.1.0

hQIOAwfq5Jrby+ZxEAf/QOdUNAhEOSfC8FD35VYqbplUXim0t02sGEakLSgPRn5hhk8kB3e1Mcqu6WN1RGXDmb0YMZapWh0oNj0syq4InrXyZMumhrCGWJwDusCH+NEQXfC4LilogaQTxKNwaF2OjRt0I7hPBrndaKhrHVC3XftK1YKwigJuFDDgKy34/5AcfU1id+R4HJucPUzz0KBOKafMpJmjVH98qgP7DWEjb5ZOimQBi7jWJF2jnYBbceFhwpL9BwtiN0yPqaZLFrZfoGAZ8HpDNV5PRgXXe6Ajekx7Jju6sZpdX2euMzOjeRC0W0QvavFkjdVXN9x2UqlQ71S3iS/bAPQCORztWQ7LIwf+JO1q7/eHg/BSuQZkI9mRXAUaslJmqZNqMmjIt1nCC2yPXYDaHEjHfMZWZycKpBPkG6QIDjNZQXgfEoA5O+wkbBWsV/cXyYw5BPECLvcmbiG4rSJ+VS06libmdpPmdOmldNWYFk+PXbh/zAAzt1GT8eBh5o9hzBdSicFNBeSZZJW9O2mQElvKJLHHry2DK1YXpfTNeK/X02nerIqGXq3S7e05klSoIc0JoKaQNzOyJBKwOa2qmG+55HKQ3ElPYM+Y3NNzP/i1nNP/oGClR6WmcuLLYrLH69fZ5rcpPHaaASTzR2g3fzYWn4cUExHRmSYNsfCfFSrdDxawpO5jwCwMYck/ZLs7dHShx9YhQDTAOvmRN6rNadrhTLBD8VZ+7pbcWfeYSTa6K68PO7a3x604MqgveVZ3tgwCIUAweveGoWQi=yIpJ

—–END PGP MESSAGE—–

But then when your patient or customers gets the email, it automatically decrypts it to deliver Ovaltine joy!

Not too complicated, right?

## **What is HIPAA Email Encryption?**

So, you get it: PHI is important. PHI is everywhere. So what do you do?

First, you need to understand the basics of encryption.

Encryption is at the heart of many of today’s data protection tools. It’s an effective way to shield data from prying eyes.

It’s not important to understand how encryption works.

All you need to know is that you start with an ultra-important secret message:

Be sure to drink your Ovaltine.

When it gets emailed out, it looks like this to anyone who tries to intercept it:

—–BEGIN PGP MESSAGE—–
Version: BCPG C# v1.6.1.0

hQIOAwfq5Jrby+ZxEAf/QOdUNAhEOSfC8FD35VYqbplUXim0t02sGEakLSgPRn5hhk8kB3e1Mcqu6WN1RGXDmb0YMZapWh0oNj0syq4InrXyZMumhrCGWJwDusCH+NEQXfC4LilogaQTxKNwaF2OjRt0I7hPBrndaKhrHVC3XftK1YKwigJuFDDgKy34/5AcfU1id+R4HJucPUzz0KBOKafMpJmjVH98qgP7DWEjb5ZOimQBi7jWJF2jnYBbceFhwpL9BwtiN0yPqaZLFrZfoGAZ8HpDNV5PRgXXe6Ajekx7Jju6sZpdX2euMzOjeRC0W0QvavFkjdVXN9x2UqlQ71S3iS/bAPQCORztWQ7LIwf+JO1q7/eHg/BSuQZkI9mRXAUaslJmqZNqMmjIt1nCC2yPXYDaHEjHfMZWZycKpBPkG6QIDjNZQXgfEoA5O+wkbBWsV/cXyYw5BPECLvcmbiG4rSJ+VS06libmdpPmdOmldNWYFk+PXbh/zAAzt1GT8eBh5o9hzBdSicFNBeSZZJW9O2mQElvKJLHHry2DK1YXpfTNeK/X02nerIqGXq3S7e05klSoIc0JoKaQNzOyJBKwOa2qmG+55HKQ3ElPYM+Y3NNzP/i1nNP/oGClR6WmcuLLYrLH69fZ5rcpPHaaASTzR2g3fzYWn4cUExHRmSYNsfCfFSrdDxawpO5jwCwMYck/ZLs7dHShx9YhQDTAOvmRN6rNadrhTLBD8VZ+7pbcWfeYSTa6K68PO7a3x604MqgveVZ3tgwCIUAweveGoWQi=yIpJ

—–END PGP MESSAGE—–

But then when your patient or customers gets the email, it automatically decrypts it to deliver Ovaltine joy!

Not too complicated, right?

## Fine, I’m drinking my Ovaltine, but why does all this matter?

Under HIPAA, there are strict rules for sending PHI over email. There are two choices:

1. You either need to be 100% sure that ONLY your recipient gets the email, or
2. You need to get permission to send insecure email AND tell them about the risks.

#2 is a hassle. HIPAA compliant email encryption is the only way to guarantee #1. Period.

If you want to send PHI over email, you need to make sure that data is encrypted.

## **So how do you send secure email?**

Like many things in life, it isn’t as straightforward as you might think. Also like many things in life, it’s a perpetual trade-off between cost and convenience. When you’re choosing a solution, think about ease-of-use in both sending and receiving. Sure, there are encryption solutions out there that are free or low cost. But they aren’t worth it if they’re going to be inconvenient or disruptive. The available solutions fall all over that spectrum.

It’s up to you to decide which one will fit your needs best. Here are a few options:

## **1) Get consent to email PHI**

In a moment, we’ll get into some more complicated encryption solutions. But first, we want to note that HIPAA actually does give patients autonomy over their own data. This means that there is one way that you can send PHI to a patient in an unencrypted email. You have to:

* 1. Inform your patient of the risks associated with sending their PHI in an unencrypted email.
	2. Get their explicit permission to with them through unencrypted email. [Here’s an example of the kind of consent form they would have to sign.](http://www.austinmedclinic.com/hipaa-and-email.pdf)

<img src="https://adeliarisk.com/wp-content/uploads/2016/08/hipaa-compliant-email-consent.png" alt="hipaa compliant email consent form" width="700" height="446" /> Be careful, though.  You have to be absolutely 100% sure that you never accidentally email someone who hasn’t opted in. Because that, my friend, is a breach. Want to explore this option? [Here’s a great article](https://personcenteredtech.com/2013/10/06/clients-have-the-right-to-receive-unencrypted-emails-under-hipaa/) that explains it in better detail.

## **2) The free options (don’t bother)**

Unfortunately, our favorite email and productivity suite (Gmail) doesn’t support sending encrypted emails. That’s a must-have when it comes to sending PHI, but it will work fine if you want to just email non-PHI. [We did find one way to send encrypted email through Gmail](http://lifehacker.com/securegmail-encrypts-your-gmail-messages-with-one-click-661685010), but it’s a huge pain. The tool, SecureGmail, requires you to give the recipient a password via a non

email method.



<img src="https://adeliarisk.com/wp-content/uploads/2016/08/secure-gmail.png" alt="SecureGmail" width="700" height="497" /> That sort of defeats the whole purpose of using email for patient communication. It may be just fine for sporadic personal use, but it’s definitely not scalable in a business setting. Your mileage may vary, but we don’t recommend it. There’s only one other completely free option, and that’s to not send PHI via email at all. You can use email for things like setting up appointments, but handle PHI only through phone calls and snail mail. Unfortunately, those are your only solutions in the $0 price range.

## **3) The heaviest-advertised option: Virtru**

Search online for “secure email,” and you’ll inevitably see the company Virtru mentioned. The [Virtru add-on](https://www.virtru.com/get-secure-email/) is easy to add to your account (though not very easy to use). Once you install it, here’s how it works: If you’re using it inside of Gmail, it looks like this:



<img src="https://adeliarisk.com/wp-content/uploads/2016/08/virtu-send.png" alt="virtu-send" width="700" height="733" /> When the patient gets the email, here’s what it looks like: <img src="https://adeliarisk.com/wp-content/uploads/2016/08/virtu-receive.png" alt="virtu-receive" width="700" height="202" /> Next, the user has to click the “Unlock Message” button. Here’s where it gets a little annoying — the user then gets another email, which supposedly verifies that this is the correct email address.  Only after clicking the second email can your user access the actual message that was sent. This double email is a double-edged sword.  On the one hand, it’s nice that they’re not making you remember yet-another username and password.  On the other hand, this “double email” approach is still pretty confusing for non-technical users (especially older patients!). On the sending side, we’ve also found that medical practices can find the add-ons (they also make one for [Microsoft Outlook](https://www.virtru.com/faq/how-do-i-get-virtru-for-my-outlook-account/)) to be pretty confusing to install.  And you have to [install yet another app](https://itunes.apple.com/us/app/virtru-email-encryption/id789957178?mt=8) if you want to send from your mobile phone.

Lastly, some of our customers have told us that the lowest-priced plan for which they will sign a HIPAA Business Associate agreement is for over $500/year, which puts them out of the reach of some small practices.  That’s not a lot to pay for HIPAA compliance, but it’s a lot to pay for just secure email.

## **4) The option from your IT company**

If you work with an IT company, they might be giving you a HIPAA email encryption add-on.  It might even be free. Companies with names like [Proofpoint](https://www.gartner.com/reviews/market/secure-email-gateways/vendor/proofpoint), Mimecast, and Reflexion primarily focus on email security.  More specifically, they protect you from phishing attacks, viruses, and ransomware emails. All of these companies are excellent at keeping your email safe (our favorite, Proofpoint, is what we recommend to clients), but they’re not that great at SENDING secure emails. Here’s how most of them work: When you want to send someone a secure email, you’ll use a keyword (like “[SECURE]”) in your subject line.  That’s the signal to the system to encrypt the email. Here’s an example in Gmail, though it looks the same in whatever email service you use.  In fact, you can even do this on your mobile phone! 

<img src="https://adeliarisk.com/wp-content/uploads/2016/08/hipaa-compliant-email-sending-proofpoint.gif" alt="hipaa compliant email sending proofpoint" width="661" height="661" /> After sending it, you’ll get a nice confirmation back: <img src="https://adeliarisk.com/wp-content/uploads/2016/08/hipaa-compliant-email-proofpoint-confirmation.gif" alt="hipaa compliant email proofpoint confirmation" width="700" height="594" /> When your recipient gets the email, it will look like this: <img src="https://adeliarisk.com/wp-content/uploads/2016/08/hipaa-compliant-email-proofpoint-patient.gif" alt="hipaa compliant email proofpoint patient" width="700" height="719" /> The recipient clicks on the “View Encrypted Email” button. Sounds easy, right? Well, not so fast.  Your patient still needs to sign up for (and remember) a username and password.  Patients can find this confusing. After they log in, they will see the secure email you sent.  They can also respond to it. 

<img src="https://adeliarisk.com/wp-content/uploads/2016/08/hipaa-compliant-email-proofpoint-patient-email-1024x478.gif" alt="hipaa compliant email proofpoint patient email" width="700" height="327" /> This one was near the top of our list, but when we tried it with medical practices, we had too many people complain about having to remember usernames and passwords.  It can work for a really small practice that almost never sends sensitive data over email, but what if you forget to type in “secure”?  It’s too easy to make a mistake.

## **5) A clunky option for Microsoft fans: Office 365**

Office 365 can send HIPAA compliant encrypted emails but, I warn you, it’s very clunky.  They’ve made some recent improvements in early 2019 which are described below, but it’s still awkward. First, [get Office 365](https://adeliarisk.com/hipaa-services/#office365). When you send the email, it looks like this:



<img src="https://adeliarisk.com/wp-content/uploads/2018/12/Office-365-Secure-Email-1024x731.gif" alt="Office 365 Secure Email" width="1024" height="731" /> See that button that says “Encrypt”?  Click that, and it’s just that easy!  After you click it, this little header will show up:



<img src="https://adeliarisk.com/wp-content/uploads/2018/12/Office-365-Secure-Email-Encrypted-1024x143.png" alt="Office 365 Secure Email Encrypted" width="1024" height="143" /> Sending a secure email on your side is pretty simple.  But when it gets to your recipient, that’s when it gets ugly. Here’s what shows up on the other side: 

<img src="https://adeliarisk.com/wp-content/uploads/2018/12/Office-365-Secure-Email-Recipient-Message-1024x750.gif" alt="Office 365 Secure Email Recipient Message" width="1024" height="750" /> When you click on that, the patient or recipient sees this: <img src="https://adeliarisk.com/wp-content/uploads/2018/12/Office-365-Secure-Email-Log-In-1024x784.gif" alt="Office 365 Secure Email Log In" width="1024" height="784" /> We’ve found that some older patients really struggle with this, and struggle to remember passwords. You also need to remember (and train your staff) about how to tell when to send a secure email vs. a regular email.  It’s really easy to forget. So while it CAN work (especially if you don’t send a lot of secure messages), it’s definitely not as easy to use as our favorite option below (#7).

## **6) Not safe for HIPAA? – SendSafely**

[SendSafely](https://www.sendsafely.com/) is another secure email service, though we wouldn’t recommend it for HIPAA email encryption. It specializes in enterprise email encryption and secure file sharing. It can integrate directly with your Gmail or Office 365 account. Alternately, you can send email through their internal portal. We’ll be blunt: we don’t recommend this option for healthcare providers or HIPAA covered entities. While SendSafely mentions that they’re HIPAA compliant on their website, they don’t mention anything about being willing to sign a HIPAA business associate agreement. Still, we’ll give you a tour of how it works ― in case you’re curious or if you’re looking for a solution for non-HIPAA reasons. After you install and activate SendSafely, here’s an example of what happens in the Gmail user interface:



<img src="https://adeliarisk.com/wp-content/uploads/2016/08/sendsafely-enable.png" alt="sendsafely-enable" width="700" height="732" /> Instead of encrypting the whole email, SendSafely just encrypts the attachment:



<img src="https://adeliarisk.com/wp-content/uploads/2016/08/sendsafely-encrypt.png" alt="sendsafely-encrypt" width="700" height="732" /> They do give you an interesting option to enable SMS verification. If you have your patient’s phone number, this could be useful. SMS verification is a great way to ensure the identity of the user. Keep it in mind if you want to go the extra mile in your email security.



<img src="https://adeliarisk.com/wp-content/uploads/2016/08/sendsafely-sms-verification.png" alt="sendsafely-sms-verification" width="700" height="235" /> On the receiving side, here’s what it looks like: 

<img src="https://adeliarisk.com/wp-content/uploads/2016/08/sendsafely-receive.png" alt="sendsafely-receive" width="700" height="352" /> Simple, right? As we said, we don’t recommend SendSafely for HIPAA-related purposes, because HIPAA just doesn’t seem to be a focus of theirs. There are better options for compliance-specific email. But it’s a good one to keep in mind for comparison or for other future uses.

## **7) The easiest, best HIPAA Email Encryption**

[Paubox](https://adeliarisk.com/paubox-encrypted-email/) is an excellent service that will automatically encrypt all of your emails. It’s, by far, the best option we’ve found for HIPAA email encryption.  You’ll need a little help setting it up. But once it’s in place, it’s definitely the easiest for both you and your patients. The best thing about [Paubox](https://adeliarisk.com/paubox-encrypted-email/) is that you don’t have to tell it which emails to encrypt.  It automatically encrypts **every email you send**. If your patient uses a modern email system like Gmail or Office365, they won’t even have to click anything. The email will appear in their inbox just like any other. <img src="https://adeliarisk.com/wp-content/uploads/2016/08/paubox-example.png" alt="paubox-example" width="700" height="154" /> Paubox uses a trick called TLS encryption to transparently encrypt every email.  Actually, over 90% of the emails sent to or received from Gmail are actually encrypted already, [according to Google](https://www.google.com/transparencyreport/saferemail/?hl=en).  [Paubox](https://adeliarisk.com/paubox-encrypted-email/) manages the rest. If your patient is using an older email system or an email system that isn’t set up the right way, however, they’ll either need to click a link or sign up for a username or password (your choice). But compared to the alternatives, this is still an extremely convenient option. Bonus: it works with Google Mail or Office 365, too.  And mobile!  Not to steal Apple’s tagline, but it’s our favorite because “it just works.”  Easy for the patient, easy for the doctor. We also really liked this service while researching this article, and decided to make it part of the solution that we implement for practices who become our clients.  [Click here if you’d like to learn more or get a price quote.](https://adeliarisk.com/paubox-great-for-hipaa/)