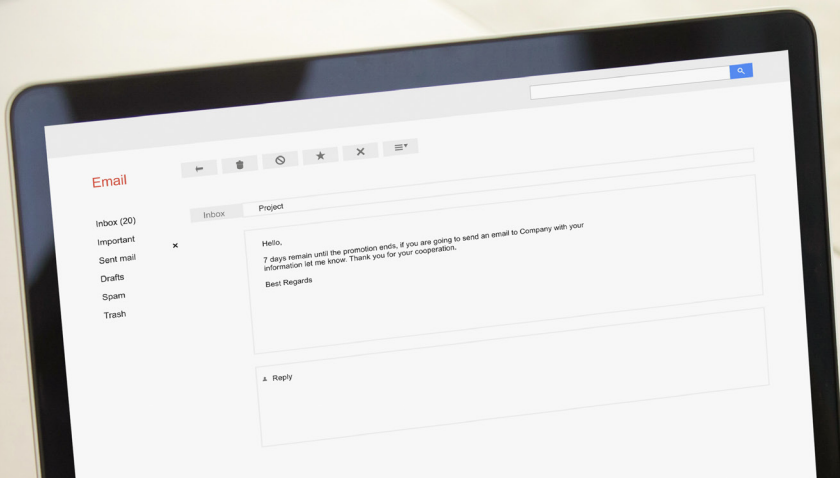


WHITEPAPER

Top five barriers to secure email communication and how to overcome them

Learn how to overcome the top five email security barriers





Abstract

An email is a ubiquitous form of information exchange. It's everywhere, and many of us can't imagine life without it. Estimates suggest that in 2020, an average of 306.4 billion emails are sent each day.¹ However, email is not in itself a secure technology. Hackers are continually stealing unsecured information, from passwords and social security numbers to birth dates and account numbers, from the river of email moving through cyberspace every second.

The healthcare industry faces particular scrutiny in securing **protected health information (PHI)**. **Covered entities** must abide by HIPAA and safeguard information according to its requirements. At the same time, allowing health information to be shared and transmitted quickly can save lives. Imagine a person rushed to the emergency room with a heart attack. Without quick access to PHI, doctors may not know what medications this patient is already taking, setting the stage for a life-threatening drug interaction. Achieving a balance between protecting PHI and allowing it to flow freely when necessary is at the heart of HIPAA.

HIPAA compliance is crucial

In 1996, the Health Insurance Portability and Accountability Act (**HIPAA**) became law in the United States. HIPAA created a set of rules and requirements for how **covered entities** subject to HIPAA, from health insurance plans to hospitals, can use individuals' protected health information (**PHI**). It requires them to protect PHI, only disclosing it in certain specific situations.² HIPAA aims to balance the need to share PHI—giving patients' medical record details to their doctors, for example—with a patient's right to keep their health information private.

¹ Lynkova, Darina. "The Surprising Reality of How Many Emails Are Sent Per Day." Tech jury. July 11, 2020. Accessed August 24, 2020. <https://techjury.net/blog/how-many-emails-are-sent-per-day/#gref>

² U.S. Department of Health and Human Services. "Summary of the HIPAA Privacy Rule." Accessed August 26, 2020. <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

How to make sure email communications are secure

The best way to ensure that your organization's emails are secure is to encrypt them using email encryption software. Unsecured email is generally sent in plain text, which means hackers can easily intercept and read messages. Email encryption uses specialized technology so that hackers are not able to read the data.

But many email encryption solutions currently on the market present significant barriers that make them difficult to use and hard to master. Here are five of the most significant barriers to secure email communications.

Email security barrier 1: clunky technology

Email encryption services use a variety of methods to secure emails. Some require email recipients to log in to a centralized portal, creating a password that they must remember in order to access emails. Others require senders to remember to use certain specific terms so that encryption “kicks in” for that email.

Email security barrier 2: substandard or incomplete training

For email encryption to work correctly—securing everything that needs to be secured—users across a company or an organization must know how to use the

solution. For many encryption tools, this requires good initial training when any new user joins the company, as well as ongoing training to refresh users' skills or apprise them of updates or changes to the way the encryption solution works. Also, if a provider does not offer blanket encryption, users need to have a strong understanding of what information needs to be secured and when.

Email security barrier 3: recipients outside the organization

Recipients of secure email, many of whom are outside the organization and not familiar with email technology, can struggle to access encrypted information.



Because time is of the essence in many healthcare scenarios, recipients can seek shortcuts or workarounds that render the security solution useless. For example, they may choose a basic password to access a secure portal, which opens it up for easy hacking.

Email security barrier 4: people make mistakes

This barrier might best be summarized as “the human element.” Complicated email security solutions are only as good as the people operating them. Senders may forget to enable email encryption, transmitting unprotected information as a result. Recipients forget passwords, meaning they cannot read emails sent to them via an email portal. Many people still

use unsecured passwords, making their accounts easy to hack.

Email security barrier 5: security theater

Security theater is the practice of investing in countermeasures intended to provide the feeling of improved security while doing little or nothing to actually achieve it.³ For many, the concept of “email encryption” is connected to portal-based or keyword-based software, both of which are difficult to use and require additional steps to implement. Because of people’s experience with these clunky technologies, many users have been conditioned to expect email encryption to be inherently difficult in order to be secure.

³Beyond fear.” Bruce Schneier. Copernicus Books. Accessed September 9, 2020. https://archive.org/details/beyondfearthinki00schn_0/page/38/mode/2up

How to overcome barriers to secure email communication

Cutting edge technologies, such as Paubox's proprietary [Email Suite solution](#), solve the problem of HIPAA compliant email communication in a secure and easy-to-use way. It removes human error from the equation by encrypting every email by default. On the recipient's side, no additional step is needed to read an email. Users simply send and receive emails as usual. When a recipient's email address does not support [TLS encryption](#), Paubox software blocks the email from being delivered in plain text and instead moves the email to a secure web app. This only adds one additional click for the recipient to view the email and ensures that you stay HIPAA compliant. Other secure email options might encrypt email—but they are not easy to use. Some providers are cumbersome to use, requiring extensive employee training. Other solutions require the sender to include a keyword, such as “secure,” in each and every email that needs to be encrypted. If the sender

forgets—even just once—security is compromised, and a [HIPAA violation](#) can result.

Organizations evaluating email security solutions shouldn't forget about the recipients—the patients, providers, payers, and other stakeholders who need to access the encrypted email's contents. Here too, many solutions fall short.

Some require recipients to download and open a suspicious-looking document. Others require recipients to create an account in order to log in to a portal, which can result in password headaches and delays. Still, others require recipients to download and install a separate plugin to receive the email. For both the sender and recipient.

Paubox Email Suite is [HITRUST CSF® certified](#), demonstrating that our solution has met key regulatory requirements and is appropriately managing risk. And unlike other solutions, Paubox is “always on,” working in the background to protect every email. Healthcare companies, large and small, trust Paubox to ensure that their organizations maintain HIPAA compliance.

Customer success snapshot: Inlusa

In one year, Inlusa, a Wisconsin-based managed care organization has used [Paubox Email Suite](#) to seamlessly and securely send more than 1.3 million emails. Implementing Paubox Email Suite has saved Inlusa's team serious time each week. Inlusa Chief Information Officer, Josh Jandrain, estimates that Paubox has freed up 20 hours a week—half a full-time equivalent (FTE). “[Paubox] wasn't nearly the support burden that the other solutions were. It was so much easier and so intuitive for everyone,” he said. “Paubox is one of the easiest products for email encryption that we've ever implemented,” Jandrain said. “The nice thing is that it just works.”

CUSTOMER SUCCESS STORY

Frontier Behavioral Health

Frontier blocks nearly 4,000 email attacks, gains an FTE with Paubox

Frontier Behavioral Health was formed as the result of a merger between Spokane Mental Health, which had been in existence since 1970, and Family Services Spokane, which was founded 106 years ago. The nonprofit organization is dedicated to working with community partners to provide behavioral healthcare to people of all ages, with a commitment to care that is both clinically and culturally appropriate.

Frontier's evidence-based approach uses trauma-informed principles and prioritizes care delivery to high-risk or high-need individuals. The organization serves about 14,000 clients each year in Spokane, WA and surrounding areas.

Company snapshot

- Founded in 1914
- 17 locations
- Paubox client since 2019
- <https://fbhwa.org/>

Paubox goals

- Free up Frontier's staff
- Have a secure and responsive email solution
- More accurately mitigate risk to the users and the agency as a whole

Experience how Paubox helps your organization get — and stay — HIPAA compliant

Start Paubox Email Suite for free

Challenge

With 750 employees, Frontier's email volume was high. The organization used an email filtering service to prevent suspicious messages from landing in users' inboxes, but it came with a significant administrative burden. Any suspicious emails were set aside, and a member of the information technology (IT) team had to review them daily.

"To manage that for 750 employees, it took one of my staff full time to go through emails and make sure the right things got through, looking through filters. Even though my team shared the responsibility for doing it, it was a pain-in-the-neck task that interfered with the team's ability to accomplish other priorities," said Paul Arguinchona, Frontier's CIO.

Solution

Paubox's suite of email security products proposed to increase Frontier's IT efficiency while keeping email secure. Frontier used [Paubox Email Suite Premium](#) to secure outgoing emails with seamless, HIPAA compliant encryption and Paubox Inbound Security to block viruses, phishing attempts, and other suspicious emails from coming into Frontier. Paubox uses [transport layer security \(TLS\)](#) encryption and is [HITRUST CSF certified](#).

"I was impressed by Paubox's ability to process emails, both coming and going more accurately," Arguinchona said.

To provide additional protection, Frontier also implemented Paubox Email Data Loss Prevention (DLP) agency-wide and used Paubox Email Archiving to encrypt archived incoming and outgoing messages at-rest. A safe record of all emails is archived, so Frontier can be assured of meeting compliance requirements or being able to initiate disaster recovery procedures right away.



"I would highly recommend Paubox. The product is very beneficial, it's solution-oriented, and it lets me sleep better at night. I'm a happy customer."

Paul Arguinchona
CIO, Frontier

“My mindset is always to protect our clients, many of whom do not have a lot of financial resources. The last thing they need is for us to fumble their information and have someone take advantage of them. That is our motivation for using Paubox’s complete email security suite,” Arguinchona said.

Results

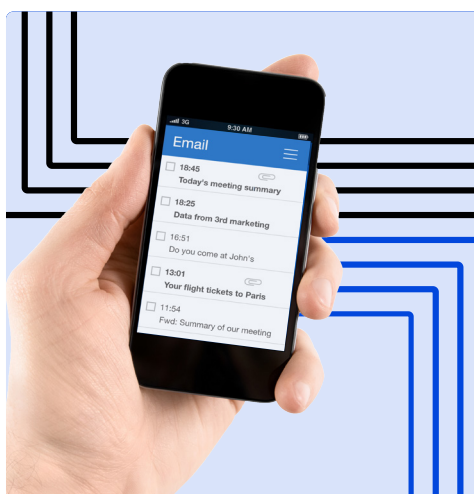
“Paubox provides a solid, consistent platform that helps me feel assured that we can get the email in that we need to get in, and that the nefarious ones will be stopped,” said Arguinchona.

Since implementing Paubox in 2019, Frontier has encrypted 192,909 outgoing emails and blocked 143,083 incoming spam emails. In addition, Paubox has stopped 2,377 viruses and 1,390 phishing attacks from landing in Frontier employees’ inboxes. Also, using **Paubox has freed up 40 hours a week for Frontier’s IT team**—one full-time equivalent—because they don’t need to manage and sift through the email filter anymore.

“I would highly recommend Paubox,” said Arguinchona. “The product is very beneficial, it’s solution-oriented, and it lets me sleep better at night. I’m a happy customer.”

Conclusion: no room for error

The costs of a breach in HIPAA compliance – both in terms of financial cost and the hit to a brand’s reputation—are immense. Removing the human element from the equation can help organizations ensure that they are protecting PHI through secure email communication. Paubox is the only solution that encrypts 100 percent of emails with no extra steps, no training, and no security gaps.



Experience how Paubox helps your organization get – and stay – HIPAA compliant

Start Paubox Email Suite for [free](#)



Paubox is the only HIPAA compliant email provider with zero-step encryption on all sent emails.

There are no portals, plugins, or extra steps to send secure data. Recipients have it easy, too, without needing to log in to a portal or set up a new account just to view a message. This makes it easy to incorporate secure email into your workflows rather than utilize a cumbersome portal-based system.

EMAIL: getstarted@paubox.com

PHONE: (415) 795-7396

