

SENDING HIPAA COMPLIANT EMAILS 101

THE SAFEST WAYS TO SEND PHI



SENDING HIPAA COMPLIANT EMAILS 101

THE SAFEST WAYS TO SEND PHI

HIPAA RULES

Snail mail is tedious. That's why email was invented, right? Unfortunately for healthcare providers, email security is a bit tricky.

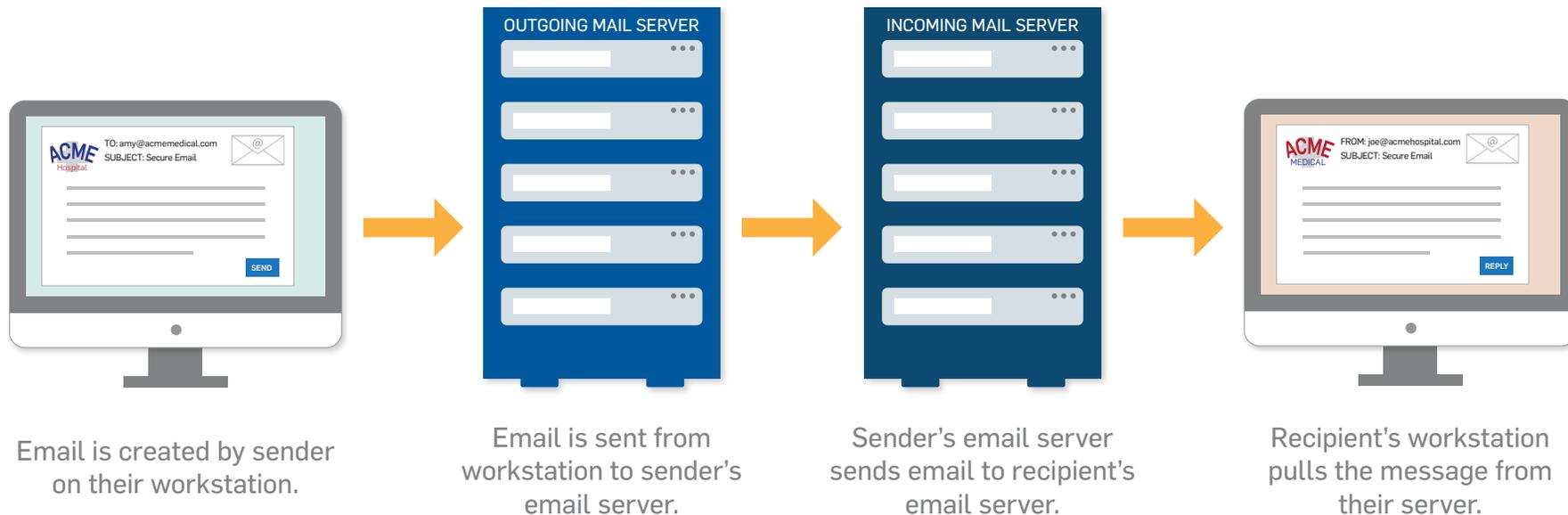
According to the Department of Health and Human Services' (HHS) Breach Portal, over 100 organization since 2009 have had Personal Health Information (PHI) stolen because of emails not being adequately encrypted and secured. Healthcare organizations need to "implement a mechanism to encrypt electronic PHI whenever deemed appropriate" such as when sending unencrypted PHI in unprotected email services (e.g. Gmail, Outlook, AOL, etc.).

Yes, organizations can send PHI via email, if it is secure and encrypted. According to the HHS, "the Security Rule does not expressly prohibit the use of email for sending ePHI. However, the standards for access control, integrity and transmission security require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to ePHI."

Essentially, you can send ePHI via email, but you have to do it securely, on HHS terms.

THE PROBLEM WITH EMAILS

To understand the reason you should secure email, it helps to grasp email transmission specifics. Typically, email follows a path similar to this:



There are a lot of links in this chain. Every time the email is sent from one machine to another, such as from the sender workstation to the sender email server, it may traverse the Internet where attackers are hidden.

A copy of the email is stored on each machine it traverses. So there is a copy on the sender's workstation, on the sender's email server, on the recipient's email server, and on the recipient's workstation.

No wonder email is an insecure way to send data. Every message may cross the Internet multiple times, plus it's stored on at least four different machines!

TRANSMISSION SECURITY

HIPAA requires that PHI remains secure both at rest and in transit. That means PHI must be protected while sitting on workstations and servers, and encrypted each time your sent email crosses the Internet or other insecure networks. Upholding transmission security significantly affects which email systems healthcare professionals can use.

There is a clear distinction between an email platform being HIPAA capable and HIPAA compliant. Most are capable, but in and of themselves, not compliant. As you can see by the path an email takes, it is pretty difficult for one product to protect that entire chain.

As a general rule, free and Internet-based web mail services (Gmail, Hotmail, AOL) are not secure for the transmission of PHI.

IN 2012, PHOENIX CARDIAC SURGERY PAID A \$100,000 PENALTY FOR NOT TAKING THE STEPS TO PROTECT DATA, AND FOR USING AN INTERNET-BASED EMAIL AND CALENDAR SERVICE FOR PRACTICE ADMINISTRATION.

If you are determined to use an Internet-based email service, ensure they sign a Business Associate Agreement (BAA) with you. Microsoft and Google recently stated they will sign BAAs. However, a BAA only goes so far, and you are still ultimately responsible. The Omnibus Rule states the covered entity is still responsible for ensuring the business associate does their part. If found in violation of HIPAA, both parties are liable for fines. The BAA typically only covers their server; you're in charge of protecting the rest of the chain.

A PATIENT'S USAGE AND RIGHTS

The HHS understands you have no control over which email clients your patients use.

"We clarify that covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email... covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual." (US Department of Health and Human Services, Omnibus Final Rule, 2013)

Basically, HIPAA rules state patients have the right to receive unencrypted emails, and as long as you use a secure email service, you aren't responsible for what happens on their end. Some caveats to remember:

- You must have another fully secure option for the patient to receive their information.
- You must still inform your patients that their email client isn't secure. If they say they still want the information, it's then permissible to send it.
- For your protection, ensure you document those conversations.



In 2 minutes, get an overview of email safety.

ADDRESSABLE REQUIREMENTS ARE OFTEN TECHNICAL, AND ALLOW ORGANIZATIONS THE FLEXIBILITY TO IMPLEMENT DIFFERENT SECURITY CONTROLS TO ACCOMPLISH THE REQUIREMENT'S OBJECTIVE.

EMAIL NECESSITIES

ENCRYPTION MUSTS

Unlike many believe, encryption does not mean password-protected. Encryption is a way to make data unreadable at rest and during transmission. Emails including PHI can't be transmitted unless the email is encrypted using either a third party program or encryption with 3DES, AES or similar algorithms. If the PHI is in the body text, the message must be encrypted, and if it's part of an attachment, the attachment can be encrypted instead.

0123 4567 8910 1112

Unlike email in transit, encrypting email at rest is an addressable requirement, which means if you don't implement it, you need to have solid documentation explaining why. But, if an unencrypted computer or laptop containing unencrypted ePHI is stolen, you will likely be fined. Look at what happened to Blue Cross Blue Shield of Tennessee, Massachusetts Eye and Ear, and Hospice of North Idaho.

EMAIL PASSWORDS

Make sure access to your email account is protected by strong passwords. For example, a password should not be found in a dictionary in any language. It should contain at least eight upper and lower case letters, numbers, and special characters. Passwords should be changed every 90 days.

EMAIL DISCLAIMERS

Email disclaimers and confidentiality notices are not a free ticket to send PHI-filled unencrypted emails. That's not their purpose. A disclaimer on your emails should merely inform patients and recipients that the information is PHI and should be treated as such. Your legal department can assist with the verbiage. The key to remember is that no disclaimers will alleviate your responsibility to send ePHI in a secure manner.

SECURING DIFFERENT TYPES OF EMAILS

IN-OFFICE EMAILS

Emails sent on your own secure server do not have to be encrypted. From nurse to doctor, office manager to nurse, surgeon to lab tech, etc. However, if you use remote access you must follow typical encryption rules. Options like Outlook Web Access can easily leak PHI, are difficult to properly secure, and should be avoided.

DOCTOR-TO-DOCTOR EMAILS

Do you have to encrypt an email if it's going to another doctor? The answer is, unless that doctor is in your office, on your own secure network and email server, YES. Remember, you are in charge of encryption during transmission.

PERSONAL EMAILS

Doctors sometimes work on cases using home computers, and then email the PHI back to their work email. Unless each of those emails is secured with encryption, this doctor just made a huge mistake. As a note to compliance officers and office administrators, if a doctor refuses to stop emailing information to his personal account, ensure you document his willfully negligent actions. Since HHS expects us to sanction employees who break policy, appropriate actions should be taken.



PROVIDERS CAN EXCHANGE EMAILS WITH PATIENTS AND STILL BE HIPAA COMPLIANT, AS LONG AS THEY ARE SENT SECURELY.

MASS EMAILS

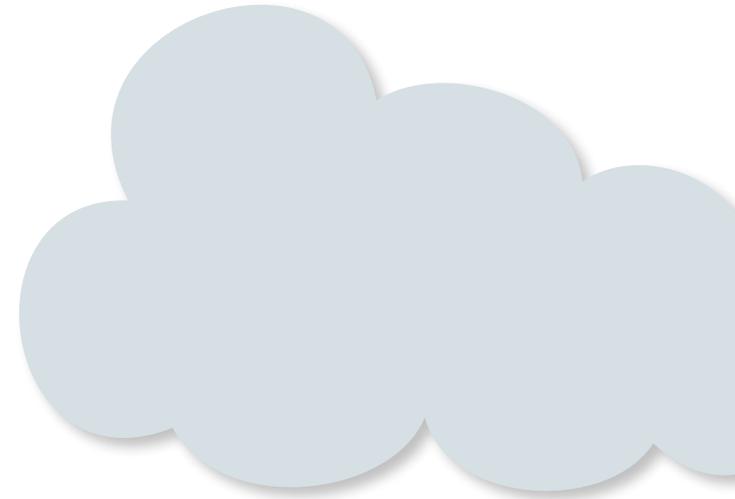
Don't send any. If you need to send mass messages, use a mail merge program or HIPAA compliant service (think business associate) which creates a separate email for each recipient. The danger of using BCC? Email addresses aren't usually hidden to the bad guys.

REPLY EMAILS

If someone replies to your email, is that communication secure? Technically, that's not your concern. HIPAA states that the entity/person conducting the transmission is the liable party. So, if the replier is not a covered entity or business associate, it's impossible for them to violate HIPAA. If the replier is a covered entity or business associate, the protection of that data is now their problem, not yours. As soon as you reply back, however, then you are again liable for the security of that transmission.

PATIENT EMAILS

How do you protect messages initiated by patients? According to the HHS, the healthcare provider can assume (unless the patient has explicitly stated otherwise) that email communications are acceptable to the individual. Providers should assume the patient is not aware of the possible risks of using unencrypted email. The provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications. Remember, you must provide alternate secure methods of providing the information to the patient.



ALTERNATIVES TO EMAIL

Due to the nature of email and the struggles to properly secure it, we recommend avoiding it whenever possible.

PATIENT PORTALS

The use of patient portals is preferred for sending information to patients, and secure file transfer options are preferred for covered entity to covered entity or covered entity to business associate communications.

Patient portals are designed for healthcare professionals to safely access their PHI online any time necessary. Not only do patient portals allow covered entities to securely communicate with other covered entities or business associates, but also patients can easily access their own information (e.g. medication information). Some portals even allow patients to contact their healthcare provider about questions, set-up appointments, or even request prescription refills.

CLOUD-BASED EMAIL SERVERS

Another route is to use a secure cloud-based email platform, such as Office365, which hosts a HIPAA compliant server. It's important to connect to the server via HTTPS so you have an encrypted connection between you and your email server. Unfortunately, this option does not control the email transmission from the cloud server to the recipient's server or workstation, so though it seems attractive, we only recommend this option when all senders and all recipients have accounts on the same cloud-based email service.

ENCRYPTED EMAIL SERVICES

Services such as Zixmail actually encrypt the message all the way from your workstation to the recipient's workstation. If the recipient is not a Zixmail client, the system will notify them of the email and the recipient can then connect securely to the Zixmail server to retrieve the message.

SUMMARY

Do not send emails containing PHI outside of your network. Instead, use secure services like patient portals. However, if you need to send emails, avoid using free Internet-based email services and make sure to encrypt all PHI in both rest and transit.

ABOUT SECURITYMETRICS

HIPAA compliance can be a complicated and time-consuming project. SecurityMetrics HIPAA services help you tackle compliance with simple steps at your own pace.

Join over 800,000 organizations and let SecurityMetrics protect your patient data.

HIPAA@SECURITYMETRICS.COM | 801.995.6801