Signs Your "Compliant" Email Service Isn't Actually Compliant (Or That It's Time to Upgrade)

By Robert McDermott; President/CEO, iCoreConnect



Cloud-based, secure email has many benefits, especially in high-security, high-compliance and high-functionality. However, to say "not all HIPAA-compliant email services are created equally" is a bit of an understatement.

Consider that security, compliance and functionality are the primary building blocks of your practice's email. They must all connect in a way that makes your workflow faster and simpler. Here's the problem. Many services show you something that looks great on the surface, but lack the infrastructure to truly improve your business. A key example is that many cloud-services claim to be HIPAA-compliant, but an unsettling number of services may only loosely meet federal law.

See if any of the following resonates with you. If so, use this information to choose a secure email service that speeds up your workflow, reduces cost and provides full HIPAA-compliance protection.

I thought spam was just annoying, but I just got hacked.

Stopping criminals at the front door is far more effective than trying to neutralize them once they're inside. Spam and phishing attacks are the primary ways cybercriminals

target medical practices, so your email service needs to stop imposters from infiltrating your PHI-relevant inbox.

The DIRECT Protocol is a standard that verifies the sender of an email is a nationally-registered healthcare provider. So it ensures your PHI-relevant inbox only contains messages from verified providers, or others you invited. The most secure cloud-based services will be built on the DIRECT Protocol, which is the federal government's preferred standard for exchanging Electronic Protected Health Information (ePHI).

It's free, and it claims to be HIPAA-compliant.

Many email services offer low or no-cost service, and claim compliance. Remember, you often get what you pay for. At the "free" level, many of these services provide encryption as the only protection. Encryption is critical, because it makes it harder for a cybercriminal to intercept and open a message that's traveling across the internet. But encryption alone doesn't cut it; it's just one of the compliance requirements. In order for an email service to be HIPAA-compliant, each of six specific federal requirements must be met.

Make certain your email service:

- Authenticates recipients using the DIRECT protocol
- Controls access with auto log-offs (and more)
- Transmits securely at 2048-bit encryption
- Keeps copies of unaltered records, storing your files in highly secure, private server centers(to prevent tampering)
- Provides an audit trail for every message, so you can produce it immediately if audited
- Securely stores your ePHI for six years to prevent damage, loss, or theft

I can't attach a large imaging file.

Hate the sight and sound of the ERROR message telling you your attachment is too big? A comprehensive HIPAA-compliant service won't restrict you to a certain size or number of files allowed in an attachment. Talk with your cloud service to make sure it offers a flexible service without file size limits at no additional cost.

I spend a lot of time logging in and out of various windows.

Here's a tip to speed your workflow. Find a cloud-based service that integrates your regular email (e.g. Gmail, Hotmail, AOL) into the same interface as your HIPAA-compliant email. One login will show you all your email options. Adding this functionality

to a robust cloud-based practice management system will mean an end to window hopping.

WMS members receive special discount pricing on iCoreExchange HIPAA-compliant cloud-based email from Friend of WMS, iCoreConnect. iCoreConnect's services are designed to speed your workflow by eliminating unnecessary steps, and reduce the cost of doing business. Contact iCoreConnect.com/wms or 888.810.7706.