eFax Corporate®

Are Your Business's Fax Processes in Compliance with HIPAA (and Other Complicated Federal Regulations)

eFax Corporate®

WhitePaper

Are Your Organization's Fax Processes Compliant With HIPAA and Other Federal Regulations Regarding Data Privacy and Security? How Can You Be Sure?

Below are 5 assumptions many large businesses make about their regulatory compliance — which are often incorrect — and strategies for correcting them.

Faxing — with its privacy benefits, ease of use and longstanding familiarity in the business world — is still a basic component in many organizations' communications processes, particularly within organizations that place a premium on protecting the confidentiality of their data and those in heavily regulated industries. In fact, faxing continues to be a growing business segment.

But ask yourself: Are your business's fax processes in full compliance with HIPAA's strict guidelines? Do they create unnecessary risks for disclosure of Protected Health Information to unauthorized recipients or employees?

Fax Compliance in a HIPAA World

HIPAA's hundreds of pages of regulations, written mostly in dense legalese, represent nearly 20 years of updates, revisions, expansions and "clarifications," from the HITECH Act to the Omnibus Rule of 2013. This has left many corporate IT executives uncomfortable answering the "Are we HIPAA compliant?" question from their senior management.

What if you could easily deploy across your organization a HIPAA-compliant cloud fax solution while at the same time help improve staff productivity, allow your employees to fax from Internet-connected devices, and save your business time and money? You can.

Indeed, in today's aggressive regulatory environment, you must. That's because in recent years The Department of Health and Human Services, through the Office of Civil Rights (OCR) and the Centers for Medicare & Medicaid Services (CMS), have stepped up enforcement, investigating more Covered Entities than in the law's first decade of existence.

Research firm Gartner Group published a study in 2012 — "As HIPAA Regulations Get Teeth, Healthcare Firms Feel the Bite" — which notes that although the law's Security Rule went into effect in 2004, it took years for regulators and the firms they oversee to fully grasp the regulations. But by 2009, after gaining years of knowledge and experience, the Department of Health and Human Services began more aggressively pursuing entities that are not HIPAA compliant. Indeed, the number of audits and enforcement has increased still further since the 2013 passage of the Omnibus Final Ruling.

Making matters even more complicated, HIPAA rules and regulations are continually being updated, requiring periodic training and re-education of staff regarding the handling of Protected Health Information. Additionally, a record number of data breaches at numerous healthcare providers in recent years has provided a sobering reminder that continual diligence in housing and transmitting Protected Health Information is required above and beyond maintaining compliance with the Privacy and Security rules of HIPAA and the HITECH Act.

Consider this…

5 Incorrect Assumptions Your Organization Might Make Regarding HIPAA Compliance (and How to Correct Them)

1. Our vendor's fax service claims it is HIPAA compliant, so our process is compliant.

An understandable misconception — but unfortunately inaccurate.

The fact that your business has deployed a solution that promises to be HIPAA compliant does not necessarily mean you are guaranteed to be in compliance with those elements of HIPAA and HITECH that the system addresses (encryption, transmission and disclosure of ePHI, for example).

Compliance with HIPAA requirements is not transferable. Although a vendor's system might meet specific HIPAA requirements, your business — as the user of that system — still needs a comprehensive overall compliance program

2. My fax provider signed a BAA (Business Associate Agreement), so I'm covered.

This is another understandable assumption. But it's also not necessarily correct.

With so much confusion regarding HIPAA, the HITECH Act and the recent HIPAA Omnibus Rule, it's important to be sure that your business and whichever vendor provides your faxing solution share the same understanding of "compliance." Even an honorable and well-intentioned vendor might be misreading the complex HIPAA guidelines and incorrectly concluding that their system is compliant.

Another important note: a BAA does not transfer responsibility from you to your solution provider. The agreement merely establishes a shared responsibility between both parties- Should you enter into an agreement with a Business Associate with whom you will disclose Protected Health Information (ePHI), both your business and the BA are 'Covered Entities' and thus held to the same Privacy and Security rules for storing and protecting ePHI under the HITECH Act, creating additional exposure for your business. Serious diligence of potential Business Associates is simply a good business practice.

3. We don't use cloud services because they are not secure.

This is no truer than concluding that onsite solutions are always more secure. Storing and securing patient data or other ePHI is predicated on strong IT security, administrative and operational controls, including periodic training of your staff. The same holds true for cloud service providers.

Well vetted cloud service providers can offer a number of key advantages — strong security, cost savings, increased efficiency, lower infrastructure overhead — over their traditional counterparts, and many offer HIPAA-compliant services tailored to the needs of healthcare customers.

4. Our corporate policies restrict user access to PHI so we are in compliance with HIPAA and the HITECH Act.

Such policies are necessary steps to take — but they alone do not ensure compliance.

While policies and procedures are key to any HIPAA-compliance program, these elements are nothing without rigorous monitoring and ongoing enforcement. You should always be on the lookout for security breaches, both technological and procedural, to ensure Electronic Protected Health Information (ePHI) is secure.

As an additional reinforcement measure, consider conducting routine training sessions with your employees regarding policies and procedures covering access and disclosure of ePHI. Additionally, performing annual Security Risk Assessments (SRAs) with a qualified healthcare IT security professional to assess risks or investigate suspected breaches is required and a good security best practice.

5. We use an in-house fax server, so our transmissions are secure behind our firewall.

This is logical but fails to consider the security of a fax server's stored data.

Yes, fax servers help ensure the security of ePHI in transmission, but what happens to that data while it's stored on your network? Fax servers often hand off data to email or file servers that could be vulnerable to unauthorized access from within the business's own network, potentially creating a reportable breach event.

As an additional layer of security, consider a cloud-based fax solution that offers "at rest" encryption of ePHI using AES 256-bit encryption. To be sure, this makes good business sense because it continually protects ePHI by making it unusable by would-be hackers.

There are no absolutes with HIPAA compliance. But when it comes to business faxing — particularly when it involves ePHI and other sensitive data — there are specific requirements your business must meet at a minimum under HIPAA and HITECH standards. And with the right solution, you can help bring your organization into compliance.

3 Features Your Fax Solution Will Need to Bring Your Business into HIPAA Compliance

1. Transmission tracking

Any faxing solution that does not offer full tracking of each fax containing ePHI or other sensitive client or patient data cannot be HIPAA compliant.

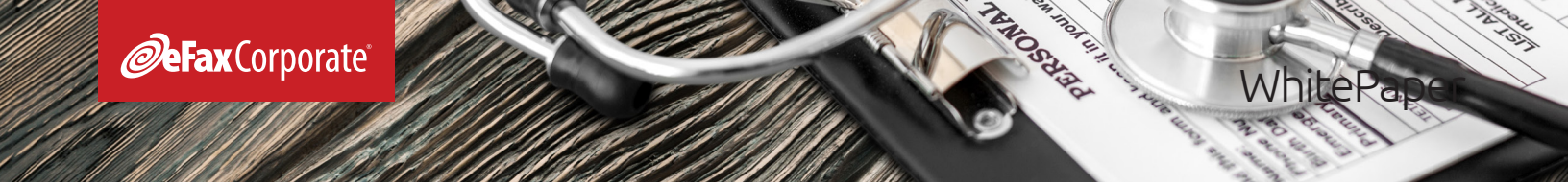
2. Transmission Security: Strong data encryption

Industry best practices show that your ePHI and other sensitive data should be encrypted not only during transmission but also while at rest — meaning while stored and archived in a digital environment and when transmitted. Specifically, transmission of ePHI should utilize enhanced TLS encryption protocol to ensure privacy over the Internet when communicating with other covered entities. When the data is at rest in the digital environment it should be encrypted using AES 256-bit encryption to enhance compliance with HIPAA regulations.

3. Digital document management and access controls

A business fax infrastructure consisting of standalone fax machines or even in-house fax servers, if not fully integrated into the enterprise's document management system, can mean a gap in document control and the inability to automate tracking and record-keeping of every fax sent and received by the business. Additionally, the ability to control disclosures to only intended individuals or covered entities enables another key control measure for ePHI and helps to mitigate the risks of sending to physical fax machines at busy office locations – which can trigger breach events.

If faxes containing sensitive data are not tracked and cataloged by your organization, with detailed records kept (and verifiable) to establish a clear "chain of custody," such a fax system cannot be HIPAA compliant.



The Solution That Offers All of These Benefits

eFax Corporate, often complemented by eFax Secure™ in the HIPAA environment, is entrusted every day to transmit millions of pages of sensitive corporate documents by businesses in the most heavily regulated industries — including healthcare, financial services and the law. Our proven process helps businesses meet the strictest federal mandates regarding data transfer, tracking and storage of Protected Health Information.

eFax Corporate®

Worldwide Headquarters
j2 Global, Inc.
6922 Hollywood Blvd.
Hollywood, CA 90028

Enterprise.eFax.com

Please Recycle