Healthcare and Secure Document Delivery

The Future of Fax

Mark D Malone

April 2018

Executive Overview

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) of 1996 turned 20 in 2016. Significant milestones speckle that timeline, one of which was the creation of the HIPAA Security Rule. The rule establishes national standards to protect electronic personal health information (ePHI).[1] As a result, standards and specifications were created so that organizations can implement compliant medical security measures. If there are data breaches for example, they may face investigations, strict financial penalties, and public exposure.[2]

Given the security and privacy directives of HIPAA, where does CBF technology fit in today's "cloudy" atmosphere for healthcare companies?

Fines and penalties: HIPAA compliance can cost companies serious money. Monetary fines can range from $100 per incident to $1.5M[3]. The U.S. Department of Health and Human Services, Office for Civil Rights, maintains a Breach Portal that lists offenders, the breach date, type, and the location of the information penetrated - among other things. A breach portal is available for public view at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Secure Fax: A safe and proven method to transmit medical documents is by fax. Decades ago, companies began to replace their fax machines with computer-based fax (CBF) systems. Over time, the use of CBF applications has become the norm for many companies, especially healthcare organizations. Document security is inherent in fax servers because of their interconnectivity with hack-proof telephone lines. CBF servers use phone lines to transmit documents using specific fax telephony protocols. Today, there are internet fax standards that embed the same protocols over the internet or a company's IP networks. Depending on the available resources, they can deploy either phone-based, internet-based or a hybrid of both.

[1] Source: U.S. Department of Health and Human Services

[2] Source: U.S. Department of Health and Human Services Office for Civil Rights; *"As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals."*

[3] American Medical Association, "*HIPAA Violations & Enforcement*": https://www.ama-assn.org/practice-management/hipaa-violations-enforcement

HIPAA and Secure Cloud Faxing: End users are transitioning their CBF systems to cloud-based fax solutions, either all or in part thereof. Offloading IT burdens and optimizing fax costs to "per usage" or volume buying models are their reasons – and this has become the goal of many healthcare organizations. "Going cloud" brings about new ePHI challenges, however. Many of the security responsibilities fall upon their cloud providers and because of that, companies must consider the risks - especially with HIPAA governance omnipresent.

Given the security and privacy directives of HIPAA, where does CBF technology fit in today's "cloudy" atmosphere for healthcare companies? This paper examines secure document delivery solutions offered by retarus Inc. and highlights their answer to the complexities of HIPAA, and their take on the future of fax.

Secure Faxing: Yesterday and Today

Computer-Based Fax (CBF via Phone/Internet)

In the beginning, CBF systems made use of the public telephone network, using analog or digital cards inside the fax server to interoperate with phone systems internally and externally. This precipitated the need to invest in dedicated phone circuits, circuit board hardware, and the telephony infrastructure. The internet has changed this model, giving users more choices. Internet-based fax ("IP faxing") standards[4] were created, and companies quickly recognized the benefits of removing fax telephony costs from their CBF investments. IP faxing still places some cost burden internally - especially when installed with IP-based voice systems.

Cloud Faxing

Today, customers can choose 100% cloud faxing options. Cloud services promise that more than just telephony costs will vanish - organizations can literally offload *all* components of their on-premise CBF system. The rapid adoption of cloud computing is skyrocketing. In 2017, an estimate placed the market at $260B and is predicted to reach **$411B** by 2020[5]. The savings and investment returns are too great to ignore and C-level executives in healthcare businesses will be incorporating cloud fax technology into their IT plans for many years to come. Now, the challenge is to implement cloud systems that meet or exceed HIPAA compliance, but what exactly defines "compliance" concerning ePHI and faxing?

The HIPAA Security Rule: Can Fax Comply?

Fax vendors, those that sell traditional or cloud, must take note of exactly how protecting ePHI is defined by HIPAA. Over the course of the last 20+ years, Privacy Rules, Security Rules, and Enforcement Rules pertaining to protected health information were defined. Ultimately, it is the *Security Rule* that provides the standards for the electronic protection of faxed private medical information.

[4] T.38 is an IP fax protocol that standardizes how faxes are transported across IP networks.

[5] Gartner News Room, October 2017 (https://www.gartner.com/newsroom/id/3815165)

"The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information (ePHI) that is created, received, used, or maintained by a covered entity."[6] The Security Rule applies to health plans, health care clearinghouses, and to any health care provider (all known as covered entities) and to their business associates[7].

Secure ePHI Document Delivery: Faxing in the Cloud

Companies are steering business programs to the cloud, and the need for securely sending fax documents has not waned – if anything it has become more critical than ever. The Security Rule itself is non-specific to fax per se. As a result, some vendors will continue to proclaim that their fax systems are "HIPAA compliant" exploiting the ambiguity prevalent during the HIPAA genesis. Today the security Rules are clearer and Cloud Fax vendors must be proficient in meeting the fundamental directives of the Security Rule broken down as: 1) Technical safeguards, 2) Physical safeguards, and 3) Administrative safeguards.

Because the obligation is placed on the end customer to be compliant, using any vendor's cloud fax service may be considered risky. However, it is the cloud fax vendors that must help their customers navigate the HIPAA maze and demonstrate what, how, and why their solution meets the customer's compliance objectives. Fortunately, there are cloud technologies that healthcare companies can deploy to minimize breaches of ePHI in a variety of digital fax settings.

> *Cloud Fax vendors must be proficient in meeting the fundamental directives of the Security Rule broken down as: 1) Technical safeguards, 2) Physical safeguards, and 3) Administrative safeguards.*

Answering Secure ePHI: Profiling retarus Inc.

One reputable cloud fax provider of note is retarus Inc. They are a U.S. subsidiary of German-based retarus GmbH who began as a services company that unified Lotus Notes email systems with online service provider CompuServe, the predecessor to AOL. They were doing this as early as 1992. From there, Retarus began offering hosted fax, email, and SMS services, and now boasts a global leadership position as a reliable provider of online fax and messaging services.[8]

The Retarus "Fax Competence Center" is in the U.S., and most of their customer business per segment are Healthcare companies and large enterprises across the country. They own and operate a secure cloud network that spans the globe, yet they have established a vast footprint within the U.S. where

[6] U.S. Department of Health and Human Services - Office of the Secretary; 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule.

[7] A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity (Source: HHS, 45 CFR 160.103).

[8] Source: Fax Over Cloud: "Commentary: retarus Inc. 21-year old global messaging company enters its 4th year operating in the United States". Mark D Malone, June 2013

customers can get service and support easily. Nearly 1/3 of their business comes from a partner channel, which is expanding, and they're experiencing a profound double-digit revenue growth at the time of this writing.[9] This is indicative of a growing Cloud Fax industry in total, and a testimony to the confidence companies are placing on it for HIPAA compliance.

retarus Inc. and the HIPAA Security Rule

As a HIPAA Business Associate[10], sensitive electronic medical data passes through the Retarus delivery network. For customers that are covered entities[11], Retarus must make sure their services enable them to adhere to the HIPAA Security Rules. Because the Rules are clear on the safeguards necessary for compliance, research data was gathered about how these safeguards match up to Retarus' services. Retarus can clearly demonstrate how they address HIPAA with a wide range of secure services.

To do this they offer secure fax and email services for Lotus Notes and Microsoft Exchange. Integrations to SAP, Windows, and a multitude of Electronic Medical Record (EMR) systems are enabled via various application programming interfaces (APIs), straightforward SMTP or even "good old" secure FTP. There is no doubt that Retarus has the right line up of cloud fax services that has come to be expected from any provider that takes ePHI seriously.

HIPAA Security Rule safeguards are defined as being "required" or "addressable" and covered entities use these guidelines to implement and ensure compliance. So, for Healthcare organizations that must protect transmitted ePHI, here is a breakdown of how Retarus responds:

HIPAA Security Rule Safeguard	Mechanisms (required or addressable)	Business Issue	Retarus Answers
Technical	**Required:** Protect ePHI, provide access to data, and encrypt to NIST standards.[12]	Data beyond the firewall cannot be breached, but if so, it cannot be deciphered. Data in transit must be encrypted.	Protects secure faxes with protocols like HTTPS, SFTP, TLS/SSL and VPN. Enforces immediate document deletion once transmitted.
Technical	**Addressable:** Implement tools for encryption and decryption	Data at rest must be encrypted.	Faxes with ePHI that would be 'at rest' can be protected via PGP, S/MIME or PDF/A.

[9] Source: Interview with retarus Inc. (S. MacDiarmid, T. Armstrong); Secaucus, New Jersey, U.S.; 01 May 2017; Mark D Malone

[10] A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Source: U.S. Dept. HHS

[11] A covered entity is a health care provider, a health plan or a health care clearinghouse who, in its normal activities, creates, maintains or transmits PHI. Source: U.S. Dept. HHS

[12] National Institute of Standards and Technology

HIPAA Security Rule Safeguard	Mechanisms (required or addressable)	Business Issue	Retarus Answers
Technical	**Required:** Activity audit controls	Logging attempted access and activity once access is granted.	Centralized control & monitoring.
Physical	**Addressable:** Physical access to ePHI, no matter what location	ePHI may end up in remote sites, over cloud networks, or remote servers.	Data center security restrictions. Logging and auditing of data. Employee data access limitations. SSAE16 and ISAE3402 certifications. Separate Telco grids.
Administrative	**Required:** Restricting third-party access	The Security Officer must ensure that ePHI is not accessed by unauthorized parent organizations and subcontractors, and that Business Associate Agreements are signed with business partners who will have access to ePHI.	Retarus employees are prevented from accessing sensitive data.
Administrative	**Addressable:** Training employees to be secure	Raise awareness about policies and procedures governing ePHI.	100% of retarus Inc. US employees are HIPAA trained and certified. Ongoing security trainings are provided.

Proof points: A Retarus Customer Interview

Industry: Healthcare Services

Revenue: > $12B (USD)
Ownership: Public, U.S. based
Employees: 50,000+
Fax Volume: 8 million pages per month, 100% Cloud-based
Fax Uses: Mostly outbound faxes, but some internal desktop fax users in remote locations

This cloud fax customer keeps three different vendors active to avoid a single point of failure, however, Retarus is their *primary vendor* and has been for over 5 years. Prior to that, they used a little-known fax vendor who is now out of business. Their end customers are doctors, clinics, and hospitals who send and receive medical faxes routinely. They have more sensitive requirements too - those that can reach life-threatening levels and they count on Retarus to have 100% guaranteed delivery. Their fax ecosystem also includes non-critical remote locations that use onsite fax servers. They plan to replace these locations with Retarus cloud faxing. In total, they send up to an impressive 8 million pages of fax per month.

> *"Their long-term strategy for secure faxing of electronically transmitted PHI is invested in the Retarus Global Network."*

The company uses a private virtual network (VPN) that "tunnels" in to the Retarus Global Network using a constantly changing 256-bit encryption. Faxes as PDF files can be encrypted to protect unauthorized viewing. On the inside, the customer's IT staff uses an internal management tool to monitor all critical fax traffic. This allows them to load balance high volume throughput as needed. Retarus delivers up to 100% "*never busy*" service through their cloud. Put it all together and conclusions can be made that this Retarus customer can in fact adhere to the Security Rule's safeguards.

This customer is serious about gauging their fax risks too. They receive periodic audit information from Retarus, combined with regular external audits they conduct separately. They even test security using "ethical hackers". It is this persistent self-evaluation that hardens the security of their cloud network and keeps their exposure to breaches and risks in check. In summary, according to the customer, their "*long-term strategy for secure faxing of electronically transmitted PHI is invested in the Retarus Global Network."*

Commentary

HIPAA rules are daunting, and taken at face value can be ambiguous, unclear, or left wide open for interpretation. Over its 20+ year lifespan, refinements to the regulations now permit covered entities to implement compliant methods to send and receive PHI electronically. The creation of the HIPAA Security Rules offers guidelines vendors deploy to implement a compliant electronic delivery system for their customers.[13] Because the rules define safeguards that are either required or addressable, there is some flexibility in how entities can deploy a solution. Retarus-specific examples of this were outlined in the included chart. As demonstrated, a properly implemented Retarus cloud network can safely transmit and receive critical PHI faxes; which means Retarus *can meet or exceed* the guidelines.

Accomplishing HIPAA compliance does not come from off the shelf cloud solution entirely. Entities must partner closely with a cloud fax provider that can accommodate their requirements. Only some vendors rise to the top; those with experience, creditably and demonstrable proof succeed. The ability to integrate enterprise systems with a variety of APIs is key, and cloud security is a must. On all fronts Retarus exhibits traits necessary to give covered entities peace of mind, backed up with proof of their network's security.

[13] "*What is the difference between addressable and required implementation specifications in the Security Rule?"* Content created by the Office for Civil Rights (OCR), 2013

Retarus' ability to integrate healthcare platforms, enterprise or legacy systems are solved using REST, SOAP, FTP, SMTP programming interfaces. The availability of these APIs, combined with a suite of standard email, Windows, and SAP integrations are draped on a backdrop of their extremely secure global network. Retarus can point to a credible list of case studies which reinforce that they can deliver a secure cloud fax service.

retarus Inc. Profile

Name: retarus Inc.	**Customer Footprint:** North America; U.K.; Europe; APAC, ANZ
Ownership: Privately held	**Largest vertical industry served**: Healthcare (approx. 24%)
Founded: 1992	**Largest customer by segment:** Enterprise (approx. 80%)
HQs: New York, USA	**Global data centers:** New Jersey, U.S.; Ashburn, U.S.; Munich, Germany; Frankfurt, Germany; Zurich, Switzerland; Singapore, APAC
Employees: 300+	**Self-stated, distinctive competency**: A secure global delivery network

About

Mark D Malone

Mark Malone has been a long-time participant and contributor in the computer-based and cloud-based Fax (CBF) industry. He began his fax journey in the year 2000 when he joined the largest worldwide leader in CBF where he remained for 7 years. Since then he has served as a Computer-based fax market consultant and market analyst, serving dozens of CBF clients. In 2012, he created Fax Over Cloud ™, a secure fax industry news site and repository for his various papers, articles, and fax product spotlights.

His high-tech career spans 28 years, 4 decades, and counting. Mark is a trained Business Analyst, a Certified Product Manager, and a Volunteer Firefighter in his local community. He is a graduate with distinction (*cum laude*), from the State University of New York at Albany.

retarus Inc.

Successful digitization, increased customer satisfaction, sustainable growth—companies reach their goals the quickest when people, machines, and applications work in perfect harmony. And reliable communication is vital for this. The better the exchange of information, the more efficient the processes. With this as the goal, Retarus steers the flow of information for major companies throughout the world.