ipswitch

Secure. Control. Perform.

AN IPSWITCH EGUIDE

7 Ways to Not Fail Your Next HIPAA Audit

How HIPAA Regulatory Requirements Apply to External Data Sharing and Are Best Addressed through Managed File Transfer

ipswitch

Introduction

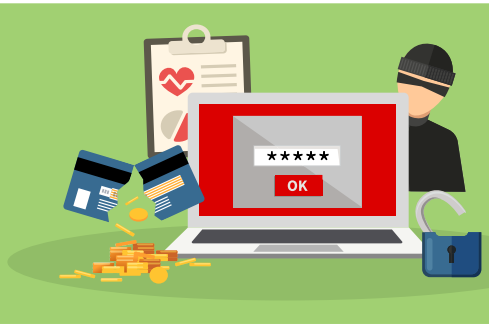
Protected Health Information (PHI) is now worth more on the black market than credit card data. This makes healthcare organizations a prime target of cybercriminals. The US healthcare industry is experiencing sharp yearly increases in both attacks and successful data breaches. In response, the government is launching a new round of HIPAA compliance audits.

The exchange of PHI with external parties is now a core operational business process of IT organizations across virtually every aspect of the healthcare industry. From a security perspective, data in transit is data at risk. Healthcare IT teams must review their exposure to attack through the tools, technologies and processes they employ to externally share protected data.

This paper addresses 7 security controls that are key to assuring HIPAA compliance in these external data sharing processes and how they translate to improvements you should integrate into your processes and tools.

The Threat

To a cybercriminal, access to PHI makes healthcare providers more lucrative targets than financial or retail institutions. Credit card data has a shelf life that lasts until the bank discovers a breach and freezes the affected credit cards. Health data, on the other hand, includes a larger wealth of information (insurer, employing company, social security, birthdate, etc), making it harder to quickly contain the abuse of using the data improperly. Health data has a longer shelf life and can be used to commit insurance fraud, buy drugs or medical equipment or steal an identity.



Personal Health Information (PHI) is worth more on the black market than credit card data.

In 2015, US healthcare organizations suffered

253 breaches

with a combined loss of over

112 million records.

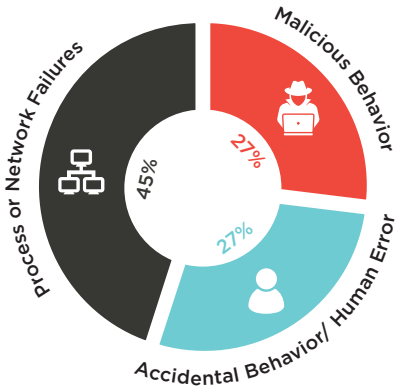
The Department of Health and Human Services' Office of Civil Rights (OCR; the US government agency responsible for HIPAA enforcement) keeps track of the number of healthcare data breaches in which the the PHI of 500 people or more is affected. The OCR reports that 253 breaches of healthcare organizations occurred in 2015, resulting in a combined loss of over 112 million healthcare records. The impact of this number is even more staggering given the 2014 census tallied the total US population at just under 320 million people.

The OCR also reports that while they issued a corresponding $6 million in HIPAA fines in 2015, this number had shot up exponentially to $15 million as of mid-2016. As a result, the government is launching phase two of its HIPAA audit program. This round of audits will be tougher than those from phase 1 which took place in 2011 and 2012. The OCR now wants to include common areas of non-compliance in the first round of audits while extending the scope to include some business partners as well.

Healthcare organizations are particularly vulnerable to data loss because they have the most valuable data, and they routinely share large volumes of that data with external partners. In a recent symposium roundtable of IT pros from New England healthcare provider networks, it was opined that as much of 85% of the information transferred to external partners was 'financial data' in the form of 835 remittance processes, government regulatory reporting and other payment provider exchanges. From a security standpoint, data in motion is data at risk and, in healthcare specifically, most of that data contains sensitive PHI which demands additional layers of protection when shared externally.

The Enemy

Causes of Data Breaches



Who is responsible for these breaches? While the media would have us believe that the predominant cause of our problems is nation states and cybercriminals, the truth is much less convenient. A recent Ipswitch survey of 255 US IT professionals showed that, against popular thought, only 27% of data breaches are the result of "Malicious Behavior". An equal percentage was blamed on "Accidental Behavior or Human Error". A staggering 45% of all data breaches were caused by "Process or Network Failures". We've met the enemy and they are us.

The truth is that most data is lost because someone within the organization or within a partner organization does something they shouldn't. This may be transmitting data through unsecured means like email attachments or consumer grade web services, or falling victim to a social engineering attack through email or social media.

Sure there are those cases where large numbers of records are stolen through advanced persistent threats from cybercriminals, but, even then, part of their attack chain usually involves unwitting insiders that make a mistake.

ipswitch

In a recent email spoofing attack, employees of a healthcare organization were asked to respond with their EFSS user names and passwords – **60% complied.**

The Response

Given that it is such a vital part of business operations, healthcare organizations need to pay particular attention to the security infrastructure, policies and governance surrounding the external sharing of protected data. The next round of HIPAA compliance audits will bring sharp focus on the security practices of both the healthcare organization itself and those of their closest partners.

The next round of HIPAA compliance audits will bring sharp focus on the security practices of both the healthcare organization itself and those of their closest partners

Your Risk Exposure

The first step in assessing your readiness for your next audit should be to assess your exposure to the risk of data loss through controlled or ad-hoc data exchanges with external parties. The three areas to examine are:

- The security of your core business file transfer processes
- The risk of ad-hoc employee transmissions of PHI via email attachments
- The prevalence/security of cloud-based file transmission

Healthcare organizations should pay particular attention to the use of unsecured file share technologies such as email, unencrypted FTP and consumer-grade cloud services by employees and external partners

CORE BUSINESS FILE TRANSFER PROCESSES

Most likely your core file transfer processes, especially those involving PHI, are already centralized to a small group of highly secured FTP servers. Hopefully, these use SFTP or FTPS which leverage SSH or SSL to assure encrypted transmission and authentication. If this is not the case, your troubles may be too large to be addressed by this whitepaper but you should definitely read on.

If this is the case, you should know that even secure file transfer processes (SFTP/FTPS) have limitations that expose you to an increased risk of security breaches and non-compliance. Key components often missing in "best practice criteria" include automation, visibility, secure tamper evident logging and non-repudiation.

ipswitch

Security/Compliance Risks of FTP include:

- **Lack of Encryption:** If the server is not SFTP or FTPS capable, file transmissions are in plain text (unencrypted) and vulnerable to theft in transit through a number of easy to use technologies.
- **Lack of Automation:** Repetitive file transfer requirements are a cumbersome process in most FTP environments leaving organizations exposed to the risk of human error and can result in significant data loss.
- **Lack of Visibility:** FTP servers lack the degree of visibility and logging required by auditors. The logs need to be tamper-evident and keep track of when a file was transferred, if it was received by the right party, and whether or not it was subsequently deleted.
- **Lack of Scale:** Organizations often rely on IT to develop a collection of home grown scripts to automate their file transfer activities. As the needs of the organization grow, the scale and complexity of maintaining of these scripts become unwieldly and can introduce unanticipated security holes into the file transfer automation algorithm.

AD-HOC FILE TRANSFERS AND CLOUD BASED TRANSMISSIONS

To maintain compliance with data protection regulations, your organization has to implement and monitor adherence to processes that assure the safe handling of PHI. A particular vulnerability IT organizations need to be aware of is the likelihood that an employee will transmit regulated data via an unsecured means such as an email attachment or via consumer grade, cloud-based file share mechanisms.

Security/Compliance Risks of Email and Cloud-Based File Share include:

- **Encryption:** Files are not likely to be encrypted both at rest and in transit
- **Distribution:** There is no guarantee that they reach the intended recipient only
- **Data Life:** Files are not deleted and data may continue to be exposed months after the initial exchange.
- **Compliance in the Cloud:** Even when cloud-based file shares are advertised as 'compliant' the transmitting company is responsible for assuring the information is secured before, during and after the transmission. Recent high-profile regulatory fines have proven it is not enough that the cloud-service itself is compliant.

ipswitch

File Transfer HIPAA Compliance Requirements

Assuring that external data exchanges are done securely and in compliance with HIPAA requires careful assessment of your current tools, technology and processes against the following seven security requirements.

Security Requirement	HIPAA Ref. Section 164	File Transfer Control
1. Compliance	308(a)(8)	Automation
2. Communications Security	312 (e)(1)	Control & Visibility
3. Information Security Policies	308(a)(a), 316(a)	Information Security
4. Access Control	308(a)(4)	Authentication
5. Cryptography	312(e)(1)	Cryptography
6. Physical & Environmental Security	310 (a, b, c, d)	Secure Architecture
7. Business Continuity Security	308(a)(7)	Failover

AUTOMATION

Commonly used file transfer workflows should be automated to mitigate against the introduction of human error that might result in data loss. Your file transfer tools should support functions such as automatic forwarding, error correction, and confirmation of receipt for all information transfers.

CONTROL AND VISIBILITY

Control and visibility of data flows and events are the most important requirements for effective security management, and essential for validating compliance. Your tools should enable central visibility, control and prior authorization of all file transfers. Logs should be kept in a tamper-evident database to assure the integrity of audit trails.

INFORMATION SECURITY

Your technology, tools or processes should ensure file integrity checks, data deletion after receipt, and non-repudiation (the sender and receiver are both authorized and authenticated to access the data). An important aspect of compliance is the existence of a tamper evident audit trail that tracks integrity, delivery, authentication, non-repudiation and subsequent deletion. This is usually established through a log database. As an extra safeguard, your systems should also prevent the recipient from altering the data, or claiming it was never received.

ipswitch

4

AUTHENTICATION

The authentication of users and administrators is an essential aspect of security and compliance. Your data share systems should be capable of accommodating an array of access control mechanisms, including integration with central user directories, role-based access control and single sign-on as well as multi-factor authentication.

5

CRYPTOGRAPHY

Encryption algorithms have a limited shelf life. Compliance standards often do not allow the use of compromised systems. It is essential therefore your data sharing systems employ strong, state-of-the-art cryptographic mechanisms and enable secure selection, distribution and protection of encryption keys, consistent with legal and regulatory requirements. To safeguard against future development of data protection regulations, your systems should ensure the continuous protection and integrity of data both in transit and at rest.

6

SECURE ARCHITECTURE

Your systems architecture should both integrate with existing security infrastructures and applications and either ensure that there is no unencrypted data within the DMZ or provide for DMZ termination of inbound requests for authentication and data transfer with a gateway proxy.

7

FAILOVER

A key requirement of many data protection regulations is secure business continuity. This requirement is meant to safeguard the confidentiality, integrity and availability of file transfers, at all stages throughout any failures, disasters or outages. Automatic, secure failover is essential to ensure that file transfers are either successful or continuously restarted until complete.

ipswitch

Ipswitch® MOVEit and MOVEit Cloud Compliance Features

MOVEit® is a Managed File Transfer system that lets you manage, view, secure, and control the exchange of sensitive data with external parties to assure compliance with data protection regulations. With MOVEit your IT team can:

- Control movement of critical data between partners, people and systems to assure data security and regulatory compliance.
- Simplify the creation of automated workflows to improve reliability, security and compliance.
- Automate performance, SLA and compliance monitoring

MOVEit Cloud is a hosted Managed File Transfer system that has obtained HIPAA compliance through annual audits by certified consultants. Ipswitch will provide a HIPAA kit to help ensure compliance along with the requisite Business Associate Agreements (BAA) to customers of this service.

SECURITY AREA	FTP SERVERS	CLOUD FILE SHARE	EMAIL SERVERS	MOVEit MFT SERVERS
Workflow Automation	◑	○	◔	●
Control and Visibility	◔	◑	◑	●
Information Security	◕	◕	◑	●
Authentication	◔	◕	◑	●
Cryptography	◑	◕	◑	●
Secure Architecture	◑	◑	◕	●
Failover	◑	◕	●	●

About Ipswitch

Ipswitch helps solve complex IT problems with simple solutions. The company's software is trusted by millions of people worldwide to transfer files between systems, business partners and customers; and to monitor networks, applications and servers. Ipswitch was founded in 1991 and is based in Lexington, Massachusetts with offices throughout the U.S., Europe and Asia.

For more information, visit **www.ipswitch.com**.

Frost & Sullivan has awarded Ipswitch MOVEit their 2016 Secure File Transfer Product Leadership Award.

In the course their industry Best Practices Research, MOVEit was found to best address the key customer and industry needs of security, flexibility and scalability while ensuring an unrivalled customer experience and ease-of-use.

ipswitch

Download your 30-Day FREE TRIAL of Ipswitch MOVEit ›