

HIPAA Compliance, Email and Text Communications

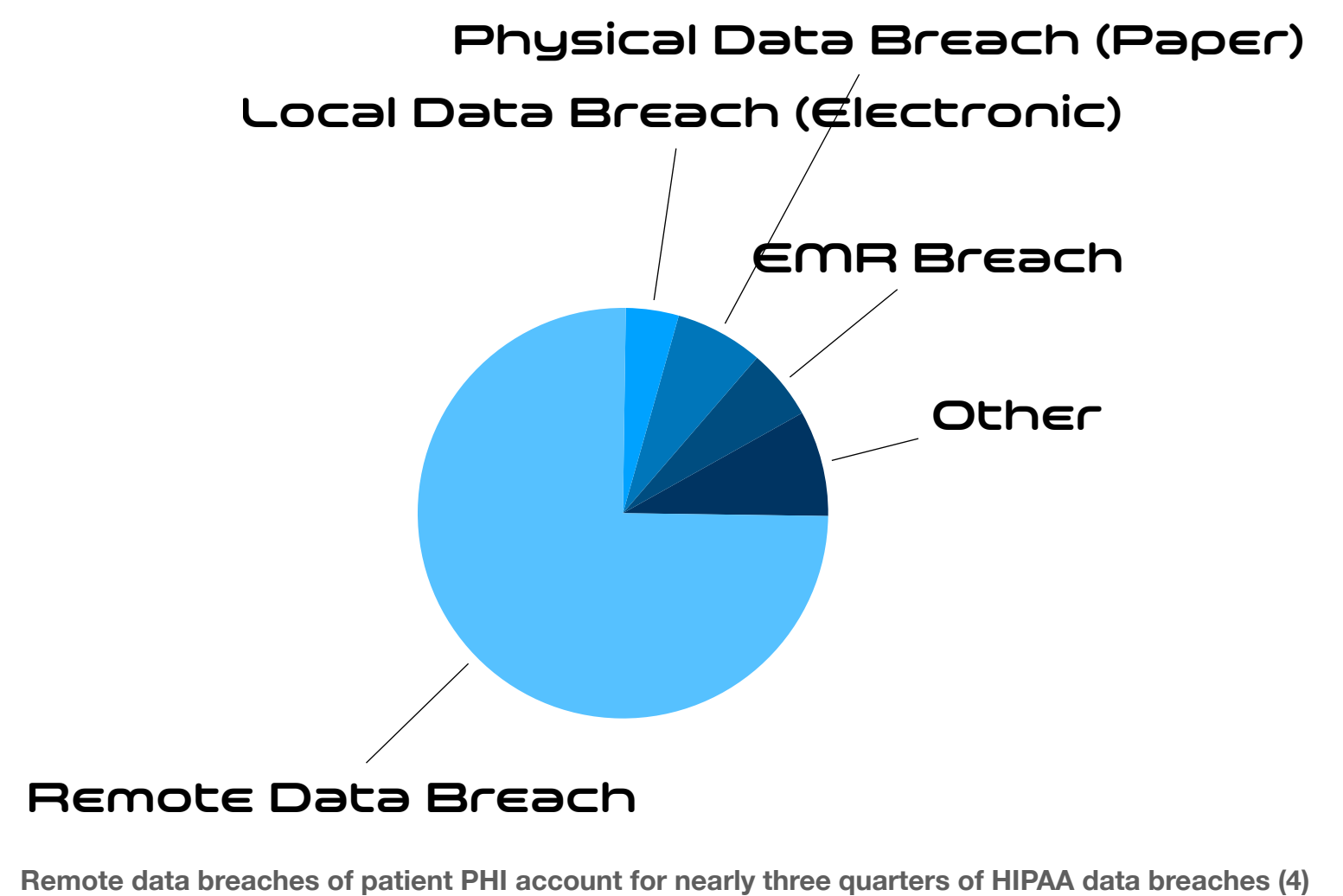
There are on average **58.8 HIPAA data breaches per month**, as of 2021. The vast majority of these breaches come from email clients and web servers being compromised by ransomware.(1)

Contrary to what you may initially think, smaller practices and clinics are often at the greatest risk when it comes to HIPAA PHI data breaches. Malicious actors look at smaller practices as being less able to deal with malware and ransomware, and thus are more likely to be targeted by hackers looking to make a quick buck.(2)

Your practice needs a HIPAA compliant means of communications that's simple and easy to use - and while the majority of health care providers now use some form of encryption to distribute information, encrypting and decrypting data can often be a cumbersome and time consuming process.

Worse still, simply encrypting data doesn't necessarily account for human error. If PHI is accidentally sent to the wrong email address, or to an email address that's shared within the household, or otherwise distributed improperly, it cannot be recalled.

Likewise, PHI is often stored in-the-clear on servers within the practice or on a Cloud service. This potentially exposes sensitive PHI to anyone with access to these platforms, making them a potential risk to the practice.



WhiteStar Chat - a New Paradigm

To combat the rise in potential cybersecurity risk for PHI, WhiteStar has created WhiteStar Chat (WSC), a HIPAA compliant messenger for Apple iOS and macOS (Apple Silicon). WSC is always-encrypted, meaning no data is ever stored in-the-clear, and data only exists locally on end devices. This means there is no potential exposure to counterparty risk should a Cloud or other remote server system be compromised.



Example:

Dec 2020 - Piedmont Health Services Hack

Cloud-based storage services can be compromised by ransomware hackers, like in the Dec. 2020 hack of Piedmont Health Services, where a Cloud server that hosted customer PHI was hacked, leaking the names, addresses, contact information, social security numbers and diagnostic codes of 81 patients.(3)

Cloud-based servers are inherently vulnerable because they present a large target to hackers. WSC fixes this problem by always keeping data encrypted, and stored locally, making the target significantly less attractive and harder to attack.



Always Encrypted - Always Secure



Encryption makes PHI unreadable to anyone without the proper keys to decrypt the information, but encryption tools are often slow and hard to use, and often patients do not understand how to use them. This complexity leads to many violations of HIPAA when providers abandon encryption for the sake of simplicity and time savings.

WSC is always-encrypted. We do the heavy lifting of making sure every piece of information sent on WSC is encrypted in flight and at rest, preventing the need for third-party encrypt/decrypt programs. Everything sent over WSC is also sent over the WhiteStar Network, which prevents sensitive PHI from being intercepted by man-in-the-middle attacks.

Integrated Document Viewing, Signing and Annotation - all in One Place

Your practice needs to be able to share and view secure, private information, and the fewer places PHI is shared, the better. In compliance with the rules of HIPAA, WSC enables users to share files, view them, annotate and sign them - all in app. This means that you don't have to worry about forgetting that you exported PHI onto your local machine - PHI that could later be compromised.

Keeping all files within WSC fully mitigates the risk of misplacing sensitive PHI and keeps all data stored under encryption.

1. <https://www.hipaajournal.com/july-2021-healthcare-data-breach-report/>
2. See source 1.
3. <https://www.thetimesnews.com/story/news/2021/03/25/data-breach-reported-piedmont-health-services/6991961002/>
4. See source 1.
5. HIPAA Journal





WhiteStar Chat

Cost and Features Comparison

	 WhiteStar Chat	 TigerConnect	 Klara
Every Chat Encrypted			
Any-Size, Any-Type Encrypted Document Exchange			
Cloudless Infrastructure			
No Data-Mining or Collection of User Data			
Does not share data with Outside Entities			
HIPAA Compliant			
Enterprise Definable Message Retention Time			
Pair-Wise Encryption			
Encryption in flight AND at rest			
No Known Security Breaches			
Real-time AI-based threat detection and mitigation			
Password stored only on local device			
Account Zeroization for User Account Deletion			

COST

8^{\$}

10^{\$.65}

8^{\$}

Setting the New Standard for Digital Privacy

WhiteStar products put user privacy first and foremost, with our revolutionary Hybrid Peer-to-Peer WhiteStar Network. The WhiteStar Network redefines the standard for digital privacy by sending packets directly between devices, keeping them out of the Cloud. This reduces the potential for PII to be compromised by a security flaw or malicious actor, reducing risk and liability.

Put another way - in comparison to apps running on the WhiteStar Network, all other communications systems put PII at greater risk of exposure.

Always Encrypted - Always Secure

Modern Smartphones are fantastic tools for productivity, but they can often have access to sensitive and private data that needs to remain private.

All content sent on WhiteStar apps is encrypted both end-to-end, and also while stored on the device. This means that sensitive information is never accessible by other apps on the phone, ensuring PII remains private.

Seamless Encrypted Document Exchange

WhiteStar Chat includes StarDrop, WhiteStar's anywhere-to-anywhere, cross device encrypted file transfer system. This enables users to send secure documents from device to device without the need to manually encrypt and decrypt sensitive files. Files sent over WhiteStar Chat and Society are stored under encryption on the user's device, meaning private files are never accessible by the phone's operating system or other applications.

Additionally, WhiteStar apps allow files, full resolution photos and videos to be shared directly in a conversation, with controllable export permissions - all without the need for the files to be stored on a third-party server or Cloud.



www.whitestarchat.io