Inside Dentistry®

eBooks

May 2017

Protecting Patient Data:

Demystifying HIPAA-compliant eCommunications

Protecting Your Patients— And Your Practice

Protecting your patients' confidential health information is of the utmost importance when it comes to sustaining a successful practice. But in an ever-evolving digital age, including many new communication options, are you as a provider doing everything possible to comply with the Health Insurance Portability and Accountability Act (HIPAA)?

Managing your HIPAA compliance protects your patients, your team, and your practice. And now, with electronic communication becoming the norm, comprehensive, consistent security is more important than ever.

RECOGNIZING THE RISK

The federal government continues to tighten its enforcement of HIPAA laws, leaving practices like yours at major risk if you and your staff aren't in compliance. The penalties for violations are staggering: One incident could put a practice out of business. Ask yourself: **Can I afford to pay $50,000 or even up to $1.5 million because an email with private patient health information got into the wrong hands?**

In extreme cases, these violations can be considered criminal acts and can lead to prosecution by the Department of Justice, complete with sentences up to 10 years in jail.

If you are currently transferring electronic protected health information across the internet, chances are your information is not safe and you are not compliant with HIPAA federal standards.

Know What to Look For

SO HOW DO YOU PREVENT ELECTRONIC MESSAGING-RELATED HIPAA VIOLATIONS?

Today, doctors cannot use the Internet to the extent that many other business professionals can because of HIPAA regulations that protect the security of patients' personal health records. You are ultimately responsible for evaluating your current communication methods, not only among your staff members but also between your practice and its patients and other providers.

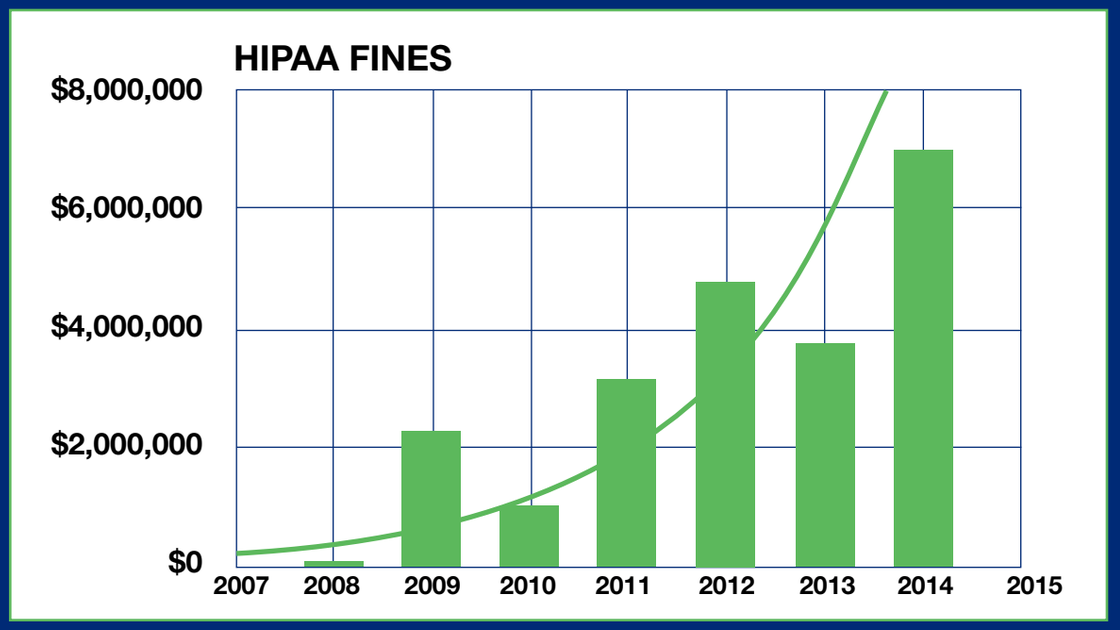
Many email and electronic messaging systems on the market today are technically secure, but they might not meet the standard of HIPAA compliance. If you or your staff members email data, lab reports, X-rays, and other protected information relating to your patients, to each other or to other dentists, you are required to make sure your email system is HIPAA-compliant.

Remember, "secure" doesn't always mean "HIPAA-compliant."

Even if you believe you're doing everything right, you need to review your systems specifically in the context of HIPAA regulations. Three of the most common email servers (Outlook 365, Yahoo Mail, and Gmail) although secure, are missing several features that are necessary for HIPAA compliance.

STEEP PENALTIES

Since 2009 the maximum fines for HIPAA violations increased from $25,000 to the current maximum penalty of $1.5 million. And there are hidden teeth in the "fine" print of the penalty structure. For each non-willful violation, the potential fine is $100 to $50,000. However, there's a potentially devastating aspect: a violation is not defined as a single data breach, or even as each patient account compromised. For the purpose of assessing penalties, a single violation is every page of protected data accessed during a breach—and fines are cumulative. In short, the fines can become staggering for even a single breach compromising large amounts of data.



Your HIPAA Compliance Checklist

THERE ARE SIX SPECIFIC HIPAA SAFEGUARDS RELATED TO EMAIL (5 TECHNICAL AND 1 ADMINISTRATIVE):

LIMIT ACCESS

1. **Access Controls:** A covered entity is required to implement technical policies and procedures that limit access to systems containing protected health information only to personnel with sufficient access rights (164.312 (a)), including having:

   a. A unique user identification
   b. An emergency access procedure
   c. An automatic logoff process
   d. An encryption and decryption process

TRACK ACTIVITY

2. **Audit Controls:** A covered entity is required to implement software that records and examines activity in systems that contain or use protected health information (164.312(b)).

SAFEGUARD ASSETS

3. **Integrity:** A covered entity is required to develop and implement policies and procedures to protect protected health information from alteration or destruction (164.312(c)). This includes having a method to authenticate protected health information.

CONFIRM IDENTITIES

4. **Person or Entity Authentication:** A covered entity has to implement procedures to verify a person or entity accessing protected health information is the one to whom the protected health information belongs (164.32(d)).

ENCRYPT DATA

5. **Transmission Security:** A covered entity is required to implement technical measures to guard against unauthorized access to protected health information that is transmitted over an electronic communication network (164.312(e)). This includes integrity controls and encryption.

STORE SECURELY

6. **Time Limit:** A covered entity is required to store and archive transmitted information in an encrypted manner, while at rest, for up to six years (164.312(a)(2)(i)).

Secure Your Chain of Communications

The U.S. government has adopted a preferred standard for eCommunication known as “DIRECT.” This is the federal standard protocol for secure messaging between healthcare providers.

- **DIRECT (data-exchange) protocol** uses a two-step verification system, checking for two unique identifiers such as a Social Security number and an ADA number.
- **DIRECT protocol** is a feature that gives a sender confidence that an email recipient truly is the intended recipient.

You need true HIPAA-compliant solutions that address current federal standards for security and interoperability. So where do you start your search for the right email system for your practice?

iCoreExchange is the dental industry expert in ePHI, conducting significant research into understanding and implementing evolving rules and regulations. Their in-depth expertise in electronic security is complemented by their extreme focus on customer support and satisfaction, a core value they refer to as being “relentlessly responsive.”

Internet hackers are continually upping their game. The bottom line is unless a practice is using an email system that is HIPAA-compliant, its providers are at risk of incurring violations and receiving penalties, fines, or jail time. Make sure you’re in compliance. Your practice depends on it.

CIVIL MONETARY PENALTIES	
TIER	PENALTY
1. Covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation	**$100 - $50,000** for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
2. The HIPAA violation had a reasonable cause and was not due to willfull neglect	**$1,000 - $50,000** for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
3. The HIPAA violation was due to willful neglect but the violation was corrected within the required time period	**$10,000 - $50,000** for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
4. The HIPAA violation was due to willful neglect and was not corrected	**$50,000 or more** for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year

CRIMINAL PENALTIES	
TIER	POTENTIAL JAIL SENTENCE
Unknowingly or with reasonable cause	Up to 1 year
Under false pretenses	Up to 5 years
For personal gain or malicious reasons	Up to 10 years

Achieving Confidence in Your System

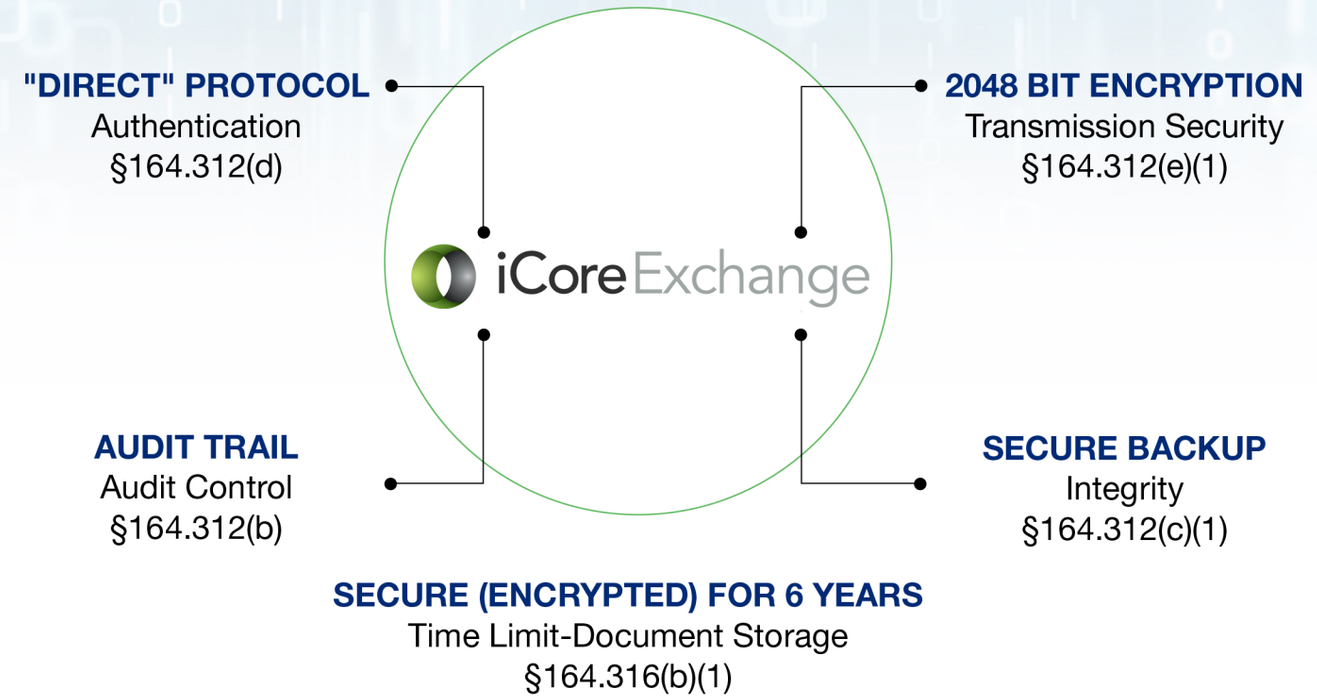
The **iCoreExchange** system allows dentists, patients, and other healthcare providers to communicate, collaborate, and exchange records, X-rays, and other protected health information, with the assurance they are in full compliance with all current federal HIPAA laws.

The easy inbox interface allows you to email anything to anyone at anytime with full HIPAA compliance. It will also let you see and use your non-HIPAA emails (such as Gmail and Yahoo) in the same inbox. The email interface is familiar and easy to use (the layout and operation of **iCoreExchange** is very similar to popular services like Outlook or Gmail). The product integrates seamlessly with most practice management, imaging, and messaging systems. Because it's cloud-based, it eliminates the need to purchase additional hardware and pay high IT costs. And you can use your HIPAA-compliant email from anywhere you have an internet connection

Do you already have a practice management system or other software platform that you are currently sending and receiving files through and do not want to change? No problem, **iCoreExchange** integrates seamlessly with most practice management and imaging (X-ray) systems.

HIPAA COMPLIANCE FOR EMAIL

5 Technical
Safeguards & Document Storage



Practice Communication with Confidence

iCoreExchange offers doctors, dentists, and other healthcare professionals the use of a HIPAA-compliant solution that addresses current federal standards for security and interoperability. As the expert in security, iCoreExchange is exceptionally responsive to its clients, helping them manage the shift to a secure, cloud-based practice management model. In addition, this game-changing software was developed with input from over 2,000 dental professionals to assure real applicability and usability in today's digital healthcare environment.

iCoreExchange PROVIDES MANY FEATURES:

- iCoreExhange is a secure, HIPAA-compliant messaging exchange and email system
- Email anything to anyone at anytime with full HIPAA compliance (patient data, lab reports, X-Rays, etc)
- Manage HIPAA-compliant and non-compliant emails from one inbox (allows you to keep your Gmail and other accounts)
- Complies with all federal and state data security regulations
- Eliminate HIPAA violations and fines associated with protected health information
- No change to your current practice workflow
- Expand your referral base by being seen by other providers looking for new referral destinations
- Allows you to collaborate with other professionals outside of your network
- Simple, inexpensive, and interoperable across most practice management systems
- Utilizes the federally-recommended NHIN DIRECT Protocol

LEARN MORE

See iCoreExchange in Action


10 HIPAA Compliance Insights for Dental Practice Email

The unfortunate truth is that not all solutions being marketed to dentists as HIPAA compliant are what they claim to be. Fortunately, you don't have to become an IT expert to get HIPAA Compliance with email right.

This white paper provides 10 important insights, presented in lay terms, to help you ensure that your practice is handling email and other ePHI correctly.

1. ePHI Compliance – Is it Really Worth It?

In a word: Yes. Aside from being a legal obligation, there are now stiff enforcement fines – up to $1.5M. Additionally, any breach must be reported to patients and the department of **Health and Human Services (HHS).** If a data breach affects over 500 patients, you have the extra responsibility of reporting to the media and your practice gets listed on the HSS website breach portal.

2. Technically Sophisticated does not mean Difficult to Use.

Expect **Ease of Use** from any HIPAA compliant email solution. Email is still the primary tool used by most practices to communicate with third parties and patients, so adding security should not complicate your practice workflow. Solutions exist that look like, and operate as intuitively as, common third party email systems like Outlook and Gmail. Imagine having a single point of sign on and management for your many email accounts, both secure and non-secure; some systems have that capability. Also, expect features like "drag and drop" for attaching files without significant file size restrictions.

3. Encryption is Key – More is Better

HIPAA compliant ePHI systems are required to meet five technical safeguards, one of which is **Transmission Security**. Encryption and decryption are critical to satisfying the Transmission Security safeguard. In the dental practice the goal of **Encryption** is to secure against unauthorized users viewing ePHI.

Ask your HIPAA compliant email provider:

- Does their solution incorporate encryption that conforms to a nationally recognized standard such as the AES (Advanced Encryption Standard)?
- What length of encryption key does their solution provide (i.e. 256-bit, 1024-bit, 2048-bit)? *Hint: the higher the number the more secure.*

In January of 2016, Henry Schein was fined $250K by the Federal Trade Commission and ordered to stop marketing the encryption for its Dentrix G5 software solution as providing HIPAA compliant level security. Their proprietary encryption methodology turned out to be far less robust than the Advanced Encryption Standard required for HIPAA compliance.

This case points out that when sharing ePHI in a HIPAA compliant manner, encryption is taken very seriously. It also demonstrates that there are email solutions being marketed as compliant that do not meet all the required HIPAA technical safeguards.

4. Sign Me Out... Please

Access Control is another of the five required technical safeguards. One vital component of this technical safeguard can be satisfied with a feature as simple as **Automatic Logoff** from workstations providing access to ePHI. The automatic logoff specification states that wherever feasible practices should:

> *"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity"*

Despite best intentions, workers may not have the time or simply forget to logoff when they leave their workstation unattended. Automatic logoff is an important feature of a HIPAA compliant system to guard against not only unauthorized viewers in the office but also remote access from hackers.

Health Information | Secure and Accessible www.imedicor.com

Whitepaper: 10 HIPAA Compliance Insights for Dental Practice Email

About The Sponsor

iCoreExchange allows any dental provider to share information with anyone at the highest levels of security, backed by highly-responsive customer support.

iCoreExchange is a national provider of secure, HIPAA-compliant communications and cloud-based practice management. iCoreExchange allows dentists, patients and other healthcare providers to easily communicate with 2048-bit encryption and collaborate with the assurance they are in full compliance with all current federal laws. All iCore healthcare applications meet the federal government's five technical safeguards for HIPAA-compliant communication.

iCoreExchange

Inside Dentistry® | eBooks

ADDITIONAL RESOURCES

Request a Demo

Sign Up for iCoreExchange (use promo code EMAILSAFE to receive 1st month free)