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.

5. "Got MicroTokenization?"

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. Here's the potentially devastating catch – 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 math gets staggering for even a single breach, compromising large amounts of data.

Enter **MicroTokenization** to the rescue. Technically speaking, unlike "Bulk" encryption where large amounts of data are encrypted together, MicroTokenization secures and protects each data element as if it were its own database with its own sets of security codes. Since every individual piece of ePHI stolen warrants its own fine, securing ePHI data with MicroTokenization adds significant protection and dramatically limits liability.

6. Do You Know Where Your Data's Been?

Audit Controls are yet another of the technical safeguards required for HIPAA compliant systems handling ePHI. Specifically, the HHS security standards guide requires dental practices to:

> *"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."*

In short, your system must be capable of tracking and reporting on who has logged in, the time and IP address of each login, and the pathway of all communications sent and received. Auditability is another advantage of cloud based solutions where ePHI never leaves the secure servers of the solution provider.

7. It's Not You, It's Them. Hardware and Server Considerations.

When you hit "send" using most email systems the message doesn't go directly to the recipient. Before reaching its destination, your message "hops" multiple times across a series of interconnected computers that make up the internet. There's no way for you to know if the devices along the way are secure, and in fact many are not.

You must keep your local servers and network up to date with the latest security protocols. Some dental offices use Outlook plugin "secure" email systems, but they suffer vulnerability from local hardware security dependency and the uncertainty of "hopping" across unsecure remote platforms. Be aware that some of these offerings are not truly secure or HIPAA complaint.

Cloud Based secure information solutions have many advantages including avoidance of server hopping and eliminating the need to purchase and maintain specialized hardware in your local environment. With the most secure cloud based solutions, your ePHI never leaves the original servers, and yet appears to the user as normal emails, with a familiar interface and all the customary ease-of-use features.

8. Be Direct

Authentication is another technical safeguard that requires the end user to verify with whom they are transferring protected information. The National Health Information Network Direct Protocol (**DIRECT)** is a federally recognized protocol developed to allow providers to communicate with identified known, trusted recipients in a secure and HIPAA compliant manner. DIRECT account holders have been vetted and certified to be who they claim to be; that is, they are legitimate to send and receive ePHI. Think of DIRECT like the TSA PreCheck service that allows validated travelers to skip security lines.

Dentists enrolled in DIRECT are readily identifiable by their email address as it utilizes the word "direct" in the naming convention. Knowing that your HIPAA compliant email system uses DIRECT provides added protection because:

1) Having the “direct.com” email extension allows you and other healthcare professionals to visually validate that the sender or recipient is sharing ePHI in HIPAA compliant manner. The HHS advises to take precautions such as checking the accuracy of email addresses before hitting “send” to avoid unintentional disclosure.

2) Penalties for violations or breaches become progressively more severe in situations involving willful non-compliance or negligence. Using DIRECT is an easy way for the government to verify that your practice has taken every reasonable measure to handle ePHI per the law.

9. Where your practice management system fits in: Interoperability

Your practice management system generates and stores a range of protected ePHI data and documents including patient birth dates, social security numbers, insurance claims, patient billing statements and clinical data such diagnoses and treatment recommendations. Your secure email system can and should provide a secure transport layer for your practice management system when exchanging EHR data with referring doctors, insurance companies or other third parties.

Interoperability means that your HIPAA complaint email solution can be easily integrated with a range of EHR systems including your practice management system. In a multi-office environment, where each office may have a different practice management system, you’ll want the same email solution to be able to “interoperate” or connect all those offices.

10. Membership Has Its Privileges

O.K. so this last point isn’t technically required for achieving HIPAA compliance with email but why not expect a little more? If your provider is certified as a privately funded **Health Information Exchange** (HIE) you can transmit ePHI in a HIPAA compliant manner across state lines without restrictions. Non-private, state funded HIE’s are limited to transferring information with that state’s boundaries. Additionally, participation in an HIE makes your practice part of a national online directory which can become an important source of referrals.

HIPAA Compliance – It’s Smart Business

Excellent solutions providing for secure email and data transfer are available for less than $40 per month. Beyond legal and financial motivations, protecting patients’ health information is good business. Long term patient relationships are built on trust; your patients care that their private health records are kept – *private*.

About the Author: *Robert McDermott is CEO and President of iCoreConnect, provider of the industry leading iCoreExchange HIPAA-compliant email solution, and iCoreDental a newly launched customizable cloud based secure EHR system. He is a recognized expert in HIPAA compliant communications, online data security, meaningful use consulting and is a frequent speaker at national and regional dental conferences.*

Prior to taking the lead at iCoreConnect Mr. McDermott has started, managed and operated six companies, three of which were ultimately acquired by major corporations. One of Mr. McDermott’s ventures made the INC 500 list and was recognized as the 173rd fastest growing company in America. He has a bachelor’s degree in finance from Dowling College, NY