Dental Managers Society Newsletter

We Welcome Medical Managers!

March 2024

Protecting Your Data: The Power of Encryption

Your business's data is like its treasure — valuable and worth protecting. Just think about all the important stuff it holds, like customer info, financial records, and secret plans. But here's the thing: there are people out there who want to steal that treasure. That's where encryption comes in — it's like a super-strong lock that keeps your data safe from thieves.

Why Encryption Matters

Encryption is like turning your data into a secret code that only you and the right people can understand. Here's why it's so important:

1. **Following the Rules:** Laws like HIPAA say you have to keep certain info safe. Encryption helps you stay on the right side of the law.
2. **Keeping Your Reputation Intact:** If your data gets stolen, people won't trust you anymore. Encryption shows you're serious about keeping their info safe.
3. **Stopping Sneaky People:** Sometimes, the threat comes from inside your own company. Encryption stops anyone who shouldn't have access to your data from getting in.
4. **Keeping the Bad Guys Out:** Hackers are always trying to break into your systems. Encryption makes it really hard for them to understand any data they steal.
5. **Bouncing Back from Trouble:** If something bad happens, like a cyberattack, encryption keeps your data safe so you can recover without too much damage.

The Cost of Ignoring Encryption

Not using encryption can lead to big problems:

1. **Data Breaches:** Hackers getting hold of your data can cost you money and ruin your reputation.
2. **Lost or Stolen Devices:** If a laptop or phone with unencrypted data gets lost, anyone who finds it can see your stuff.
3. **Inside Jobs:** Sometimes, employees can cause trouble by taking sensitive data. Encryption stops them from doing harm.
4. **Getting in Trouble with the Law:** Breaking data protection laws can mean big fines and legal trouble.

How Encryption Works

Encryption turns your data into a secret code. There are two main types:

1. **Symmetric Encryption:** It's like using the same key to lock and unlock a door — efficient but you have to be careful with the key.
2. **Asymmetric Encryption:** This uses two keys: one for locking and one for unlocking. It's safer for sharing data.

Continued on page 3

Letter from the Editor

Pam Snell,
DMS Advocate

Happy Spring!

Although this is meteorological spring and the weather has been warm and cold in turns, I've yet to see any signs of spring life — crocuses, daffodils, forsythias, or other signs of spring life.

We were just talking about what a difference it is from four years ago! On Monday, March 16, 2020, our world went upside down as we helped clients go into lockdown and work from home. We were doing the same thing; David and I were the only ones working in the office while our team supported our clients from their homes.

Today, most dental practices are very comfortable logging into their office computers from home, and it's very productive. But in 2020, they had no clue, and we walked them through all the steps and helped them feel secure.

Although we are prepared for almost any disaster, we hope we never have to go through anything like that again!

Are you taking advantage of all the FREE services that we offer?

I've been updating the ***DentalManagersSociety.com*** website with lots of advice from our Team of Experts. Be sure to check it out! Along with the Experts' posts, here are some other features:

- **David's 95.9 WATD radio spot:** Every Tuesday morning at 8:11, David joins 95.9 WATD's The South Shore's Morning News host Rob Hakala for our Tech Talk segment. We spend about 8 minutes talking about what's new or alarming in the technology industry that could affect your practice and your life.
- **Our Monthly Infographic:** Read it and request a copy be mailed to you.
- **Our Weekly Video Tech Tip:** Quick, easy to understand, and helpful information.
- **Free Reports** such as "The Top 10 Cyber Risks to Your Practice and How to Avoid Them"
- **Our monthly newsletters,** past and present.

ACTSmart's motto is to "Help You Benefit From Today's Technologies"!

The Dental Managers Society website and newsletters are ways that we are accomplishing that.

Stay Healthy, Happy, & Safe!

Continued from front page

Using Encryption for Your Business

There are different tools for different jobs:

1. **Locking Files and Folders:** Built-in tools on your computer or special software can help you lock up your files.
2. **Securing Emails:** There are programs that can encrypt your emails, so only the right person can read them.
3. **Protecting Whole Devices:** Tools like Bit-Locker or FileVault can keep your whole computer safe.
4. **Keeping Cloud Storage Safe:** Some cloud services can encrypt your data before it even leaves your computer.
5. **Making Communication Secure:** Using things like SSL/TLS or VPNs can protect data sent over the internet.

Best Practices for Encryption

To make sure encryption works well:

- Use strong passwords for your encryption keys.
- Keep your encryption keys safe.
- Update your encryption software and teach your team how to use it.
- Encrypt your backups, too.
- Test your encryption regularly to make sure it's working right.

Choosing the Right Encryption

Pick the type of encryption that fits your needs:

- Think about how sensitive your data is.
- Make sure it works with the other software you use.
- Check to see that it meets any legal rules you have to follow.
- Make sure it's easy for your team to use.
- And make sure it'll keep working well into the future.

In short, encryption is like putting a lock on your data to keep it safe. By using it right, you can keep your business safe from all sorts of trouble.

Are Managing Vendors Eating into Your Practice’s Valuable Time?

You have an incredibly important job that keeps you very busy. On top of seeing patients, continuing education, and maintaining an organized, thriving practice, vendor management can seem like a thankless extra chore.

In truth, vendor management can be the more tedious side of business that has little to do with the work that you love, takes more time than maybe it should, and can be frustrating and confusing to no end. However, if you’re not on top of it, there’s a good chance your practice could be leaving money on the table.

There’s no shortage of vendors you must deal with.

Dentists, dental office administrators, and anyone else in charge of operations at your practice have to keep track of various vendors to ensure the smooth operation of their practice. These include, but are certainly not limited to:

Dental supply companies – who provide materials and consumables such as gloves, masks, branded oral care equipment for your patients, and more.

Office supply companies – who provide everyday necessities like paper, ink cartridges, pens, folders, etc.

Software and eSignature vendors.

Telecom services vendors.

Payment processing and integration vendors.

Compresses gas vendors – for your nitrous oxide and other gas cylinders.

General, medical, and shredding waste disposal companies.

Altogether, expenses like these can add up to around 20-30% of your budget, and that’s no small chunk of change.

Balancing your expenses with your time.

So, we can agree that 20-30% isn’t an unimportant figure. But what can you do about it? Your expenses are your expenses, right? Maybe not.

You don’t have to – and shouldn’t – take your vendor rates as written in stone. In fact, when you think about it, there’s a very good likelihood you’re paying more than you should. You only know what *your* practice pays; your vendors know what all their clients pay, as well as what their competitors are charging. There’s an information imbalance, and it’s not in your favor.

In order to prevent overpayment, you do have to be vigilant and do frequent analyses of your expenses. This includes steps like:

Regularly reviewing your invoices, contracts, and plans to ensure everything is aligned and meets your practice’s needs.

Negotiating with your providers for better rates or discounts.

Investigating whether services can or should be consolidated under one vendor.

Utilizing appropriate expense management **software** to keep track of things like supply deliveries and charges.

No one likes staying on hold with telecom companies for hours or reading over the sometimes hieroglyphic-like invoices they receive from their payment processor. It takes time away from your important work and doesn't always lead to clarity. However, without appropriate intervention, you're letting your vendors decide whether they can over-charge you.

In conclusion…

One of the biggest challenges facing any dental practice these days is a lack of hours in the day to do everything that needs to be done while providing high-level services to patients. While you may already feel stretched thin, vendor management isn't something to deprioritize. If you do, it could eat into your revenue, make your practice less profitable, and prevent you from reinvesting money back into your staff and services.

Introducing Bryan Berry

Delivering businesses greater profitability by reducing their monthly expenses and adding to their bottom line.

SCHOOLEY MITCHELL

Bryan Berry | Strategic Partner
Tel: 781-427-9595 | Cell: 508-479-7190 | Fax: 781-499-9177
40 Bayberry Circle | Bridgewater | Massachusetts
www.schooleymitchell.com/bberry
bryan.berry@schooleymitchell.com

HIPAA and Ransomware-Be Prepared!

The "Ransomware" term strikes fear into the hearts of any business owner or manager, particularly in dental or medical practices, which have significant amounts of private information they cannot by law be allowed to release to unauthorized individuals.

Imagine that all your practice computers are frozen, infected with malicious software (malware), and a message comes over your system that states quite menacingly that all your practice and patient information is in what appears to be an unknown criminal's hands, and that there is an unbelievably high ransom demanded to decrypt and release and return it.

Not only is this a serious breach of the HIPAA statute but the ransom for returning the computers to normal and allowing access to information may easily be in the thousands or tens of thousands of dollars. And who knows if the ransom is actually paid that the kidnappers will return all the protected health information without keeping it for their own use and further demands.

This kind of ransomware attack has been made on dental practices, and the Department of Health and Human Services (HHS) and Office of Civil Rights have come out with a fact sheet on Ransomware and HIPAA to give covered entities under HIPAA guidance on preemptive steps to take to avoid a ransomware attack, and what a practice should do in case of an attack..

First, the HHS makes it clear that a ransomware attack is very likely a HIPAA breach and an unauthorized release of Protected Health Information (PHI). This security incident must be reported to the HHS and patients since it may affect large numbers of patients and may be a release to suspicious unauthorized individuals, which could cause harm to affected patients.

The answer to that question is determined by reference to the HIPAA rules on breach incidents that a HIPAA Privacy Officer (which very practice must name) must go through for every breach that is recognized by the practice.

- What was the scope of the incident (what identifying information was compromised of how many patients)?
- Who was the release to (ransomware entities are criminal enterprises)?
- What is the chance that the PHI was acquired or viewed (was it encrypted enough to lessen the possibility that it was viewed and is the risk ongoing)?
- Has the extent of the risk been mitigated (can recovery efforts contain the release and forestall risks of more releases or future ransomware efforts)?

Of course, every practice should have an IT company that has expertise in handling these kinds of incidents to consult with on how to respond immediately as well as how to recover the systems affected back to a "business as usual" status.

An IT expert may help with the decision about the risks of actually paying a ransom (which is almost never recommended), the potential exposure, recovery actions, and how to prevent ongoing and future attacks.

The HHS makes it clear that following existing rules for HIPAA risk management and risk analysis, already required under HIPAA to be conducted regularly and at a minimum, annually, can help prevent and mitigate the risks of a damaging ransomware attack.

Brian Hatch
Hatch Legal Group
8 North Main Street, Suite 403, Attleboro, MA 02703
HatchLegalGroup.com
brianhatch@hatchlawoffices.com

Risk analysis includes many factors, including how PHI is encrypted, how networks are isolated, and training personnel on how to detect malicious software or preventing a more serious infection when that malware is detected. There should be training on recognizing suspicious forms of infection they realize have already occurred.

Entities should have a written security incident response plan that is included in the risk assessment and management analysis required by HIPAA. Sometimes just awareness of what a "phishing" request is for PHI can prevent employees from responding to such suspicious inquiries (like from unrecognized entities, often with misspellings, grammatical errors, or unusual e-mail addresses).

Controlling and restricting internet use in the workplace to only required actions for performing one's duties can be effective to preventing malware from attaching, considering that the internet is a prime source of ransomware attacks.

HIPAA rules require post-incident actions, which can protect against future security incidents such as ransomware attacks.

There are requirements that privacy officers conduct post-breach analyses of HIPAA breaches and how to manage risks and prevent breaches in the future.

A written risk management plan is required under HIPAA audits and annually there must be evidence of a risk management analysis.

Isn't is amazing that just following HIPAA rules, which sometimes seem overly burdensome, can prevent the real-life nightmare of a serious ransomware attack?

ACCESS TO YOUR FILES AND PRIVATE DATA HAS BEEN LOCKED.

Enter your payment details to to gain access.

$300 USD / €250 EUR

YOUR DATA WILL BE DELETED IN:

23:12:01

NOW!

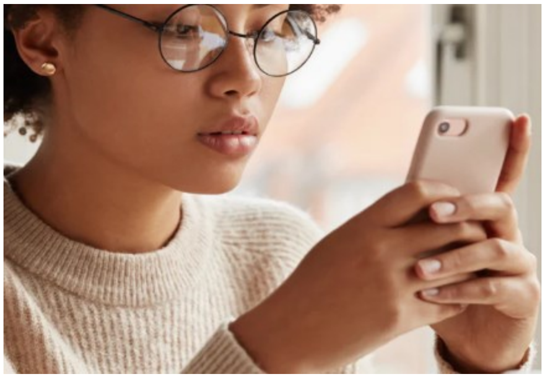
Dental Managers Society—Sponsored by ACTSmart IT
332 Main Street
Wareham, MA 02571

In This Issue:

This newsletter was thoughtfully edited by Susan Rooks, the Grammar Goddess, so we can look and sound as smart as we are.

Susan Rooks
The Grammar Goddess
508 272-5120
SusanR@GrammarGoddess.com

Manage Patient Reviews & Improve Online Reputation with Weave



What Patients Look for in Reviews

When reading through your facility's online reviews, patients look for a few key aspects. The top factors patients consider include the following:

Bedside manner: Did the doctors have a compassionate and empathetic bedside manner toward the client and family? Did your team listen to patient needs and explain things clearly?

Office environment: Is the office clean and organized? Was the front desk staff friendly, attentive, and able to direct the patient to their needs? How long was the wait time?

Staff behavior: Did the staff behave in a positive, helpful way? Does the staff seem as though they've been through adequate specialty training? Was the patient able to schedule their future appointment or surgery date without a hassle?

Patient care: Were the patient's needs met? Did the provider clearly explain their treatment plan, providing health tips and protocols for the next visit?

Book a Demo. No onboarding fee when you sign up through ACTSmartIT.com/weave

weave Authorized Partner