Patient Information Protection Compliance Is Not a Small Deal

Understanding the serious risks of not being truly compliant with HIPAA and PCI-DSS regulations

arevtech
Managing Technology | Enabling Success

MISTAKE #5 Not complying with PCI-DSS and HIPAA regulations for patient information protection

Patient Information Protection Compliance Is Not a Small Deal

Understanding the serious risks of not being truly compliant with HIPAA and PCI-DSS regulations

An annual study by ID Experts and Ponemon Institute on the privacy and security of healthcare data has highlighted some alarming results. In 2016, nearly 90% of healthcare organizations surveyed had experienced a data breach in the past two years. Almost 79% had two or more data breaches in that timeframe. That's an increase of almost 20% since the first study in 2010.[1]

The cost of those breaches is estimated at **$6.2 billion.**

If you don't think the healthcare industry is more susceptible than other industries, think again. According to a 2015 annual report by Symantec, almost 40% of all data breaches took place within the Health Services sub-sector. And 36% of all data breaches (across all industries) included medical records.[2]

In addition, a 2016 study by the Identity Theft Resource Center (ITRC) confirmed the significant vulnerability of the healthcare industry:[3]

- **Healthcare organizations were hit hardest by hacking, skimming, and phishing attacks.**
- **Healthcare organizations had the most records exposed by employee error or negligence.**
- **Healthcare organizations exposed more social security numbers than any other industry (including business, education, financial, and government).**

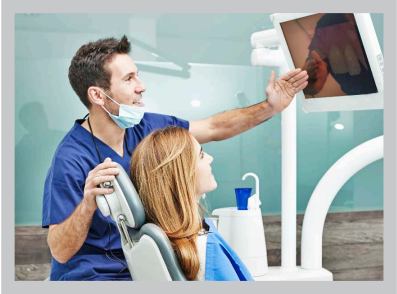
PCI-DSS and HIPAA compliance matters

The harsh facts simply emphasize how critical it is for your dental practice to properly protect your patient data and comply with the Payment Card Industry's Data Security Standard (PCI-DSS) and the government's strict Health Insurance Portability and Accountability Act (HIPAA) regulations.

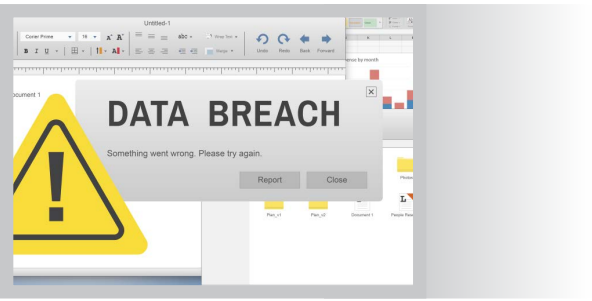
If you haven't already done so, you need to assess your practice and answer some vital questions (with honesty):

- How certain are you that your own current IT infrastructure includes the kind of advanced data protection controls and monitoring necessary to accurately comply with PCI-DSS and HIPAA regulations?
- Do you truly understand the requirement for encryption as HIPAA defines it?
- Are you properly adhering to the numerous HIPAA regulations that specifically address data backup and recovery requirements?
- Is your backup data encrypted, stored off-site, and tested on a regular basis?
- Are you certain you'll be able to restore any lost data?
- Do you perform regularly scheduled security assessments of your entire IT systems?
- Are you certain that only specific, authorized people can access patient information? Are you accurately logging which employees have access, and when they access the data?
- Is your practice audit-ready?

The Protenus Breach Barometer Report indicated that 2016 averaged at least one health data breach per day, affecting more than 27 million patient records.[4]



The stakes are high if your patient data is breached



The financial losses for data breaches are staggering. Over a two-year period, the average cost of the patient data breaches experienced by healthcare organizations **was more than $2.2 million per healthcare organization.**[1]

But the costs go deeper than the financial losses. Data breaches are truly devastating for practices.

You are required to immediately notify all of your patients in writing of the breach. You must also notify the local media to publicly disclose the breach. Furthermore, your practice will be listed on the website of the U.S. Department of Health and Human Services as a practice that has had its data breached.

How many of your current patients will you lose? What will it cost you, and how long will it take to win even half those patients back? How many new potential patients will rule out your practice as a safe, viable option? Can your dental practice even survive such a disaster?

Noncompliance with the Payment Card Industry Data Security Standard (PCI-DSS) could result in fines levied by banks and/or credit card institutions ranging from $5,000 to $500,000 per month, depending on the payment brand and nature of noncompliance.[6]

Even if your practice is 100% PCI compliant and validated, a breach in cardholder data may still occur that could result in a fine of $50–$90 per cardholder's data compromised, suspension of credit card acceptance by your credit card account provider, and a potentially serious loss of reputation and trust with patients, suppliers, and partners.[6]

There's serious personal risk, too

Failing to comply with HIPAA can result in both civil and criminal penalties. Enforced by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), civil penalties are monetary and can go up to $1.5 million per offense depending upon the type and severity of the violation. Criminal penalties are enforced by the U.S. Department of Justice, and can result in up to 10 years in jail. [5]

And breaches of credit card data caused by a lack of compliance with PCI-DSS requirements can also result in civil action by your patients or suppliers.[6]

Don't worry. There's help—and we're called Arevtech.

If all the risks involved with patient information protection compliance are scaring you, that's normal. But the good news is, there's professional help with the proven expertise and solutions designed to protect dental practices from these risks—and help ensure compliance with both HIPAA and PCI-DSS. And that's Arevtech.

At Arevtech, we have years of experience delivering the protections needed to help ensure that your IT systems are compliant with PCI-DSS and HIPAA—while keeping your dental practice audit-ready. We perform regularly scheduled security assessments of your IT systems as part of our Regulatory Compliance Services. To best support you with a start-to-finish compliance solution, Arevtech partners with compliance experts for all administrative and non-IT related compliance services—helping to ensure your practice is truly compliant, safe, secure, and confidently protected from a data breach.

Peace of mind—and more

Besides helping safeguard your practice and ensure regulatory compliance through our Regulatory Compliance Services, our experienced Managed IT Services offers 24/7 network monitoring, giving you peace of mind knowing that Arevtech has deep insight into your network. This allows us to keep your critical systems and network up and running, secure your vital data, and address IT issues before they become real problems.

arevtech
Managing Technology | Enabling Success

Contact Us Today

Contact us today to learn more about how Arevtech's team of experts provides friendly, knowledgeable IT service to help you build and grow a streamlined, productive practice while enabling you to stay focused on providing top quality patient care.

714.256.1500 Talk to one of our Dental Practice IT experts, or visit us at **www.arevtech.com/Dental**

NOTES:

[1] ID Experts, **"Six Years Later, Patient Data Still at Risk for Data Breach,"** June 2016.

[2] Symantec, **"ISTR Insights: Cyber Threats and the Healthcare Industry,"** June 2016.

[3] Healthcare Informatics, **"Report: Healthcare Sector Hit Hard in 2016 by Data Breaches,"** January 2017.

[4] Healthcare Informatics, **"Healthcare Data Breaches: A Year in Review,"** January 2017.

[5] American Medical Association, **"HIPAA Violations and Enforcement."**

[6] Focus on PCI, **"PCI Noncompliant Consequences."**

ADDITIONAL REFERENCES:

Dentistry IQ, **"The dark side of HIPAA compliance: 3 things health-care providers should know in 2016,"** June 2016.

Dental Products Report, **"Is your dental practice completely HIPAA compliant?"** January 2015.