TROJANTODAY
The Newsletter for Today's Dental World
Volume 26, Issue 9

IN THIS ISSUE

The Risks of Outdated Hardware and Software in the Dental Office

by JoJo Jackson

In today's digital age, dental offices increasingly rely on technology to manage patient records, streamline operations, and enhance the quality of care. While this technological advancement has revolutionized the industry, it has also introduced new challenges, particularly cybersecurity and compliance with privacy regulations like the Health Insurance Portability and Accountability Act (HIPAA). One of the most critical aspects of maintaining a secure and efficient dental practice is ensuring that your office's hardware and software are up to date. Failure to do so can lead to operational inefficiencies and pose significant security threats that jeopardize your business and your patient's personal data.

What Are the Risks

Outdated hardware and software in dental offices can create significant vulnerabilities that cybercriminals are quick to exploit.

(CONTINUED ON PAGE 2)

Here are some of the potential risks associated with not maintaining up-to-date technology:

- **Security Vulnerabilities:**

  Older software versions often contain security flaws that have been discovered and patched in newer releases. Without regular updates, your systems are exposed to cyberattacks, including ransomware, malware, and phishing schemes.

- **HIPAA Non-Compliance:**

  HIPAA mandates that all healthcare providers, including dental offices, protect patient information through secure and up-to-date technology. Failing to update your systems can result in non-compliance, leading to fines, legal consequences, and damage to your reputation.

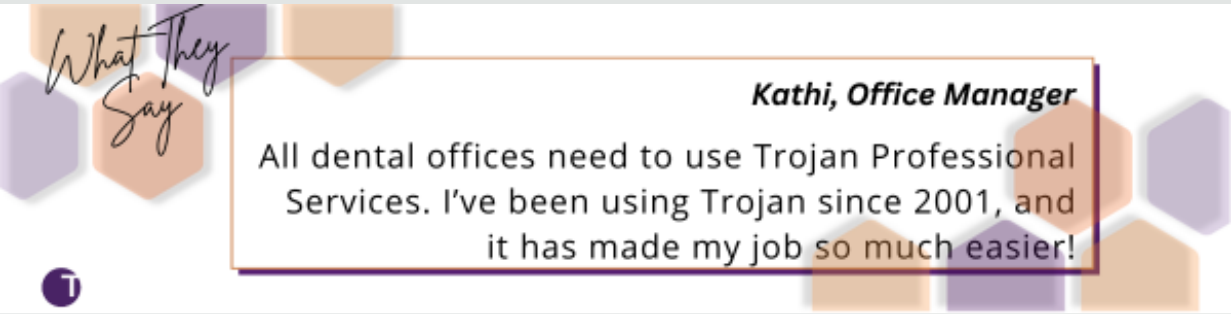
- **Operational Inefficiencies:**

  Outdated hardware can slow down daily operations, causing delays in patient care and frustration among staff. Additionally, older systems may not be compatible with newer software, leading to further complications and increased downtime.

- **Data Loss:**

  Older hardware is more prone to failures, which can result in the loss of critical patient data. Without proper backups and security measures, recovering this data can be costly, time-consuming, and sometimes impossible.

(CONTINUED ON PAGE 3)



Ensuring HIPAA Compliance: Steps to Take

It is essential to prioritize the maintenance and updating of your technology to reduce these risks and ensure your dental office remains HIPAA compliant. Here are some actionable steps to help you achieve this:

- **Conduct Regular Security Audits:**

  Regularly review your office's hardware, software, and security protocols to identify vulnerabilities. This audit should include an assessment of your network, servers, computers, and any other devices that store or transmit patient data.

- **Implement a Patch Management System:**

  Ensure that all software, including operating systems, dental practice management software, and third-party applications, are regularly updated with the latest security patches. Consider using automated patch management tools to streamline this process.

- **Upgrade Hardware as Needed:**

  Assess the condition and performance of your office's hardware regularly. If your computers, servers, or network devices are outdated, consider upgrading to newer models that offer better security features and performance.

- **Encrypt Patient Data:**

  Encryption is a critical component of data security. Ensure that all patient information stored on your systems is encrypted at rest and in transit. This includes emails, patient records, and any other sensitive data.

(CONTINUED ON PAGE 4)

- **Train Your Staff:**

  Educate your team on the importance of cybersecurity and HIPAA compliance. Regular training sessions can help staff recognize potential threats, such as phishing emails, and understand the importance of following security protocols.

- **Backup Data Regularly:**

  Implement a robust backup strategy that includes regular backups of all patient data. Ensure that backups are stored securely, preferably offsite or in the cloud, and that data can be quickly restored during a data loss incident.

- **Work with IT Professionals:**

  Collaborate with IT professionals who specialize in healthcare to ensure your systems are secure and compliant. These experts can guide the latest security measures and assist with implementing new technologies.

(CONTINUED ON PAGE 5)

Check out these seminars and online and training opportunities:

Christine Taxin's
Dental Extravaganaza 2025

Rebecca Gerber
https://www.dentalpracticecareers.com/

Ask the Consultant

Answer by Kathleen Johnson

Q: Do HMO plans require treatment preauthorization? My patient has an HMO as their primary and a PPO as their secondary. What is the process for treatment preauthorization for this type of dual coverage? The treatment includes fillings, crowns, and implants.

A: Preauthorization for managed care dental plans is only for specialists.

Generally, PPO plans do not require a preauthorization for restorative procedures. It is your choice to verify the plan benefits for major dental procedures, such as implants to be sure of your estimates.

Advocate for HIPAA Compliance in Your Dental Office

As a dental professional, it is crucial to advocate for HIPAA compliance and the security of your patient's data. Here are some ways you can be an advocate:

- Lead by Example: Prioritize security in your work to demonstrate the importance of HIPAA compliance. Adhere to best practices and stay informed about the latest developments in cybersecurity to show your team that you are committed to protecting patient data.
- Promote a Culture of Security: Encourage a culture of security within your office by regularly discussing the importance of cybersecurity and HIPAA compliance. Make it clear that protecting patient data is everyone's responsibility.
- Invest in Training and Resources: Provide your staff with the training and resources to stay informed about HIPAA compliance and cybersecurity. Consider hosting regular workshops or bringing in experts to educate your team.

(CONTINUED ON PAGE 6)

- Stay Informed: Keep updated on the latest developments in healthcare technology and cybersecurity. Attend industry conferences, subscribe to relevant newsletters, and network with other professionals to stay ahead of potential threats.
- Advocate for Change: If you notice areas where your office could improve its security measures, speak up. Advocate for the necessary changes to ensure your office remains compliant with HIPAA and that patient data is secure.

Conclusion

Integrating the latest hardware and software in dental practices is not just a matter of efficiency but a critical component of patient data security and HIPAA compliance. Dental offices must proactively update their technology as cyber threats evolve to safeguard sensitive patient information from breaches and unauthorized access. By ensuring that systems are regularly updated, encrypted, and backed up and by fostering a culture of security awareness among staff, dental practices can decrease risks and maintain patient trust. Compliance with HIPAA is

not just about avoiding penalties; it is about upholding the ethical responsibility to protect patient privacy in a digital age.

Maintaining up-to-date hardware and software in dental offices cannot be overstated in an increasingly digital world. Ensuring that your practice is HIPAA compliant and protected against cybersecurity threats is essential to safeguarding your patient's data and the success of your business. By following the steps outlined above and advocating for a culture of security, you can help ensure that your dental office remains a safe and compliant environment for your patients and your staff.

ABOUT THE AUTHOR

JoJo Jackson is the Software Support Supervisor and has been with Trojan Professional Services for 11 years.

FMI: www.trojanonline.com

“Quote-Worthy

It takes 20 years to build a reputation and a few minutes of a cyber incident to ruin it.
-Unknown”

SEPTEMBER 2024 VOL. 26, IS. 9

Three Reasons to Schedule Your Free Training

Staff Turn Over

Take some of the stress out of training and new staff member. You are not only doing all the work yourself but you are also taking extra time to teach someone else how things are done in your office, have them start with a Trojan Training.

Do you have team members who have never had a free professional Trojan Training?

Long Time Client and New Features

You may already be familiar with what we do, but at Trojan, we constantly improve based on your feedback. We want to ensure you understand the new products and services available to current clients. Do you know…

- We have a Learning Center
- Ask The Consultant is included in your monthly fee
- Your desktop eligibility program saves your patient's information forever
- About the 6 Trojan Guidelines for finding Trojan Benefit Plans faster
- The research fee is per plan, not per patient
- We have an automated eligibility service called Dentifi that automatically processes eligibility for your patients nine days in advance and every day up to 24 hours in advance.

A free professional Trojan Training can show you all these services.

Call us today at 800.451.9723 ext. 1. Or, visit www.trojanonline.com, click APPOINTMENT CALENDARS, then TRAINING.

TROJAN PROFESSIONAL SERVICES

Accelerating dental practices to excellence by providing services that increase case acceptance, production, collections, and profit.

TROJAN TODAY PHONE: 1-800-451-9723 • E-MAIL: nikkim@trojanonline.com • www.trojanonline.com • Published monthly by Trojan Professional Services, Inc., P.O. Box 1270, Los Alamitos, CA 90720 and distributed to members of the dental profession. Statements of opinion in TROJAN TODAY do not necessarily reflect the opinions of Trojan Professional Services, Inc. or the Editor. Neither Trojan Professional Services, Inc., Trojan Today, its Editor, nor its staff assumes any liability in connection with the use or implementation of any policies or procedures discussed in this newsletter. Trojan Today is distributed as a newsletter, with the understanding that neither the publisher, the Editor, nor the staff render professional or legal services of any kind. If legal or professional advice of any other kind is required in connection with topics discussed in this newsletter, competent advice should be sought.
• PRESIDENT: Ingrid Kidd Goldfarb • EDITOR: Nikki Myers •