APEX

Publication of the Stanislaus Dental Society

Winter 2019

HOW SAFE IS YOUR PRACTICE?

Data breach

Ransomware

Website security

Data security

Content

Articles

Backyard

Published by the
Stanislaus Dental Society
Mailing Address:
2401 E. Orangeburg Ave.
Ste. 675-319
Modesto, CA 95355
Physical address:
2339 St. Pauls Way
Modesto
Ph: (209) 522-1530
Fax: (209) 522-9448
Email: sdsdent@thevision.net
Website: stanislausdental.org

Questions or comments about the content of this publication may be directed to:
Editor: Charles Kim, DDS
Editorial Manager: Robin Brown

Your contributions in the form of articles, photos and/or ideas are greatly appreciated. The APEX editorial staff is interested in articles of general membership interest. This can include an accomplishment, interesting hobby, innovative idea, volunteer effort, etc. Please feel free to submit an article or call for an interview. All articles are subject to editorial review.

Presidential Pondering

Dr. Amanda Farley, SDS President

Insurance. We all need it. We all have it. Life, disability, business overhead policies, business owner policies, workers compensation, EPLI, and many more. What happens when you need to exercise the policies you pay for monthly? Which policy would be most appropriate for which situation? Do you have gaps in your policies and are there loopholes that you need to be aware of? Let me help you understand a few little know (hopefully generally known) provisions to be aware of for your insurance woes.

Life: Provides security for loved ones in unexpected loss. Additionally, can cover student debt, business debt, can be used as collateral for business purchases. Many banks will not approve a business loan for a burgeoning entrepreneur without collateral like life insurance. Don't let your student debt keep you from your business ownership goals.

Disability: With the right provisions in your policy, you can have complete or partial disability coverage in addition to the right to your "true own occupation". You can be injured from your occupation as an endodontist, collect your full disability benefits and transition into another career. Most plans will cover through and sometimes past age 65 and have negotiable waiting periods to collect benefits.

Business Overhead: Allows for partial or full business overhead coverage in the event you are disabled or incapacitated for a period of time. It will allow for you to be able to keep the practice running while you recover or transition your business.

Commercial Business Owner: Employee, patient, independent contractor, temp hygienist or dentist coverage for injuries on your property or related to your business. It also covers building coverage and everything under its roof. Not to mention it can cover cybercrimes, accounts receivable, employee dishonesty and more.

Employment Practice Liability: Employing people can be difficult and it is not without its challenges. EPLI coverage will cover lawsuits and complaints with claims related to wrongful termination, harassment, and unfair treatment. Be aware the most policies will not cover wage complaints and labor board complaints.

Worker's Compensation: If you employ anyone, this is a must. Obviously, it will allow coverage for workplace related injuries. In the case of some policies, it can provide prevention programs to help promote safety and prevention.

TDIC has new grad policy discounts available for whatever your needs may be early in your career. As we mature into our careers, TDIC also offers multi-policy discounts to incentivize bundling your policies together. Though TDIC is one of the most popular carriers, do your research with your broker as other companies can offer similar discounts as well as comparable coverage.

As tempting as it can be, make sure you are not shopping strictly based off your premium prices. The "cheap" policies may have hidden provisions that may make your life harder after the fact. Speak with dental specific broker regarding policies. They know how valuable "true own occupation" provisions and more can be essential in our line of work.

(continued page 4)

2019 SDS Officers

President
Amanda Farley, DDS

President-Elect
Victor Pak, DDS

Treasurer
Samer Hamza, DDS

Secretary
Eric Dixon, DDS

Editor
Charles Kim, DDS

Trustee
John Sulak, DDS

Immediate Past President
Dean Brewer, DDS

2019 Committee Chairs

Bylaws
Matt Swatman, DDS, MSD

Community Health
Gloria Fass, DDS

Continuing Education
David Walls, DDS

Ethics
Matt Swatman, DDS, MSD

Forensic Odontology & State Emergency
Garry L. Found, DDS

Legislative
Andrew P. Soderstrom, DDS

Media Relations
Elizabeth Demichelis, DDS

Membership
Eric Dixon, DDS

Peer Review
Jennifer Leon-Guerrero, DDS

Program
Victor Pak, DDS

Well-Being
Michael Shaw, MD, DDS

Toll Free Numbers

ADA. . . . (800) 621-8099
CDA. . . . (800) 232-7645
TDIC . . . (800) 733-0634
TDSC . . .(800) 253-1223
Denti-Cal Referral
…….(800) 322-6384

(continued from Page 3: Presidential Pondering)

Bottom line: Being a dentist is expensive. Secondary bottom line: it can be even more expensive without the appropriate insurance coverage. Know your policies, ask your brokers what your terms and provisions are. It's like I tell my patients - if you don't trust the opinions you are getting and do not feel comfortable with the answers to the questions you are asking, keep searching for the answers that make you secure if your decision. It is our job as providers to inform our patients about all risks, benefits and alternatives. Why shouldn't we hold our brokers and insurance providers to the same standards? Keep this in mind as you review the policies you hold, and I hope that you can use these words of advice to shore up your protections and safety nets.

Meet the Newest SDS Board Member in 2020, Secretary David Walls, DDS

Dr. Walls is both a physician and dentist with specialty training in oral and maxillofacial surgery. He is board certified in oral and maxillofacial surgery and has active medical and dental licenses.

Dr. Walls was born and raised in Nashville, TN. He completed his bachelor of arts in economics and philosophy at Columbia University in New York and attended dental school in Nashville at Meharry Medical College School of Dentistry. He then returned to New York to earn a degree in medicine at New York University School of Medicine and a general surgery internship at NYU. He completed his and oral and maxillofacial surgery residency at NYU where he was trained in the full scope of the specialty including general anesthesia and surgical care for both adult and pediatric patients.

Dr. Walls has a continuing interest in the most current practice of oral and maxillofacial surgery with a focus on dental implant surgery, bone graft reconstruction of the jaws, pathology including jaw cysts and tumors, and facial trauma surgery. Dr. Walls has also presented at the American Association of Oral and Maxillofacial Surgeons Annual Meeting. He has privileges at Doctor's Medical Center and Memorial Medical Center in Modesto.

Dr. Victor Pak gifting outgoing President Dr. Amanda Farley with a plaque of appreciation. Thank you for your years of service on the board!

(l to r) Incoming Continuing Education Chair Jeff Barton, Trustee John Sulak, Editor Charles Kim, President Amanda Farley, President-Elect Victor Pak, Treasurer Samer Hamza, Secretary Eric Dixon, Bylaws and Ethics Chair Matt Swatman, Incoming Secretary David Walls

Trustee Report

by John L. Sulak, D.D.S.

In October, the CDA Board of Trustees discussed a number of items. Highlights of the meeting included:

Board Composition Task Force Recommendations: The board composition task force was established in 2018 to evaluate the board structure and make recommendations to assure board members possess the necessary skills and reflect the diverse experiences and perspectives required to achieve organizational goals. Over the past two years, the task force has worked closely with the board of trustees, providing potential options for consideration. The trustees provided valuable feedback to the task force based on their board experience and component needs, which helped shape the final recommendation: the creation of a 32-member component relations board of advisors and establishment of a 16-member board of directors, which was approved by the board in October, for further consideration by the House of Delegates. Trustees are urged to speak with their delegates regarding this recommendation and to encourage them to attend one of the upcoming pre-house educational sessions, which will provide an overview of the recommendations and allow delegates to ask any questions they may have prior to the meeting.

Dental Benefits and Economics Task Force Recommendations: In fulfillment of the 2017/2018 house directives, the dental benefits and economics task force addressed dental insurance and practice economic issues to make recommendations as to how CDA can assist members in responding to the ever-changing environment. The board approved the proposed recommendations, which have been incorporated in the task force report. Dr. Viren Patel, task force chair, will present the report during the educational house sessions Friday morning, after which the house will be asked to file the report.

Medicare Task Force Report: In 2018, the house directed CDA to form a task force to explore issues relevant to the inclusion of dental benefits in the Medicare program, including implications in California on the aging population and the delivery of care. Over the past year, the Medicare task force gathered information from several sources and experts; received background information on the national and California health care environments and Medicaid and Medicare programs; obtained data on aging Californians and other relevant materials as identified; and engaged in a detailed analysis of potential benefit approaches and multiple considerations. The board received an overview of the task force findings, which Dr. Gary Herman, task force chair, and Dr. Marko Vujicic, ADA chief economist, will present during the educational house sessions. Following, the house will be asked to file the task force report.

- 2020 CDA Budget: The board approved the 2020 budget, which will be included in the financial overview during the house.
- CDA Postgraduate Discount: The board adopted a recommendation from the council on membership to change the postgraduate discount, providing a 100% discount to new graduates.
- Executive Director Management Objectives: The board approved revisions to the executive director's 2019 management objectives and established the 2020 management objectives.
- Editor Evaluation and Objectives: The board approved the editor's 2019 evaluation and 2020 objectives, retaining Dr. Kerry Carney as editor for 2020.

(continued on Page 6)

(continued from Page 5)

- Establishment of Editorial Board: One of the editor's 2019 goals was to explore and evaluate opportunities to update CDA publications. Through this work, it was identified that an editorial board was an effective and expedient mechanism for continuing to improve publications for CDA members. As such, the board approved the proposed editorial board as recommended by Dr. Kerry Carney.
- CDA 150th Anniversary Program Funding: Next year marks CDA's 150 anniversary, setting the stage for a renewed way to increase brand awareness, promote the mission and purpose of the organization, honor its history of innovation, celebrate tradition and articulate the vision of the future. The board received a presentation on how CDA plans to commemorate this anniversary, engaging CDA members in a unique way. Following the presentation, the board approved funding for the anniversary program.
- CDA Website Redesign: The board also received an overview of the newly designed cda.org, which will be released via a soft launch in November 2019

TDSC Update: The board received an update regarding the TDSC.com out-of-state expansion. This discussion was held in closed session as it contained proprietary information that is not appropriate to discuss externally due to the competitive nature of TDSC's market. However, the board can share that TDSC will be national, across all 50 states by year-end. TDSC has affiliation agreements with 37 states, with five more expected within the next 15 weeks. Additionally, TDSC will close the Lynwood distribution center effective Nov. 30, at which time all orders will be fulfilled through the Reno center or through TDSC distribution partners.

In addition to these discussions, the board received a number of emerging issues presentations focused on the potential MICRA initiative, federal health care landscape in Washington and expansion of oral health care in dentistry. The board also approved funding to support CDA's participation in state and federal health care issues through 2020, including federal advocacy and policy support. Sincerely,

John L. Sulak, DDS
CDA Trustee

The objective of the Stanislaus Dental Society shall be:

"To encourage the improvement of the oral health of the public, to promote the art and science of dentistry, to encourage the maintenance of high standards of professional competence and practice, and to represent the interests of the members of the dental profession and the public which it serves.

Cyber Security in 2020 and beyond

by Charles C. Kim DDS, SDS Editor

As we quickly approach the new decade, it would be best to strengthen our knowledge and secure our offices even better to protect our patients and all of us. With high tech development, we live in society even a light bulb is connected to the internet via Wi-Fi. Unfortunately, anything and everything connected to the internet can be hacked. Hackers used to exclusively pursue financial institutions. As time went on, they are targeting larger and larger amounts of personal information including health information accumulate and make sales off of all the data they wrongly collected. Let's talk about the main cyber threats and how to minimize such threats.

Email phishing attacks are becoming commonplace where it is used to trick us to give our information. Usually posed as an email sent from a larger company asking you to verify or extend the services by logging into a website in an email link could be deleted before it is opened. If the sender's email is not authentic, don't attempt to click anything and just delete the email. Some major company also has phishing reporting accounts where you can forward this email to report them.

Ransomware attacks involve malware that denies the user access to files until a ransom is paid. Even after the ransom is paid, you can be assured that your data won't be released. The best type of practice is installing and keeping up to date on antivirus software on all computers in the office as well as updating operating systems. Especially windows users must update their operating system to Windows 10 by the end of this year as the support for Windows 7 is being terminated on January 14, 2020.

Lastly, loss or theft of equipment, as well as data loss, either intentionally or unintentionally must be avoided at all costs. Encrypted backup regularly as well as offsite backup of such backup must be a routine process. Physical and cybersecurity measures should be outlined and trained to all personnel to prevent a data breach.

Many companies help with all of these for a monthly fee ranging from $100 up to $1000 with most of the companies charging around $200 per month. However, before you sign up with any of such services, it is recommended that you consult your current IT support and go over what the current status of cybersecurity protections are and how to keep it up to date to best protect our patients and us.

Want to save more on supplies than you pay in dues?

There's no better time to be an association member! Your benefits now include big savings and free shipping on dental supplies and small equipment through **The Dentists Supply Company**.

Get the most value from your membership by leveraging collective buying power for your own practice.

SHOP ONLINE AND START SAVING TODAY

tdsc.com The Dentists Supply Company

FAQ: How to Manage Windows 10 Updates

by Ed Bott for The Ed Bott Report

This article has been updated multiple times since its initial publication. The most recent update was September 5, 2019, and includes details about important changes that were effective with version 1903.

With Windows 10, Microsoft has completely rewritten the Windows Update rule book. For expert users and IT pros accustomed to having fine-grained control over the update process, these changes might seem wrenching and even draconian.

You can't pick and choose which updates to install? There's no option to delay updates on PCs running Windows 10 Home? Upgrades to new versions are mandatory?

Welcome to Windows as a service.

The new update rules are designed to solve some nagging problems in the PC ecosystem. For example, if every user can choose some updates and reject others, the number of potential configurations approaches infinity; Microsoft argues that all those untested variations make effective quality assurance much more difficult.

Likewise, Microsoft's generous 10-year support lifecycle has enabled fragmentation in the installed base: Over the past decade, Microsoft's engineering staff have been required to support as many as five major versions at the same time. In a world where security challenges arrive at breakneck speed, that stretches support resources to the breaking point.

And thus a new approach to Windows Update, whose goals are to have the majority of Windows users fully patched at all times, with only a few versions to support and an installed base that is mostly running one of the two most recent versions. But pushback from frustrated customers has resulted in some major adjustments in 2018 and 2019.

This FAQ covers the details you need to know, especially if you're the administrator in an unmanaged environment.

WHAT KIND OF UPDATES ARE AVAILABLE FOR WINDOWS 10?

Microsoft provides two types of update packages for Windows 10:

Feature updates are the equivalent of what used to be called version upgrades. They include new features and require a multi-gigabyte download and a full setup. Each version update gets a major version number that corresponds to its date of release, in the *yymm* format, as well as a build number that identifies it. Version 1709, for example, was finalized in September 2017 and is identified as build 16299. Microsoft's schedule is to deliver Windows 10 feature updates twice a year.

Quality updates address security and reliability issues and do not include new features. These updates are cumulative, and they increment the minor version number after the major version number. The January 2018 cumulative update for version 1709, for example, is 16299.192. Even if you skip several months' worth of updates, you can install the latest cumulative update and you will be completely up to date.

All available security and reliability updates are included in a cumulative update and cannot be selected or rejected individually. That's a major change from previous versions and a big surprise to anyone upgrading to Windows 10 for the first time.

Besides these cumulative updates, you might see servicing stack updates delivered separately. These update packages fix issues in the code that Windows 10 uses to scan for and process updates. Security updates for Adobe Flash Player and definition updates for Windows Defender are also delivered as separate packages, not included in cumulative updates.

Hardware drivers and firmware updates can be delivered through Windows Update. Typically, these packages are provided only when the driver fixes a bug that causes instability on targeted systems.

(continued on Page 10)

(Continued from Page 9)

HOW ARE UPDATES DELIVERED IN WINDOWS 10?

For consumers and small businesses, both quality and feature updates are delivered via Windows Update. Organizations can use internal update management solutions, such as Windows Server Update Services, to distribute updates to computers on a corporate network.

Feature updates are made available to business and home editions of Windows at the same time. (Until 2019, there were separate *servicing channels,* also called *branches*, for home and business customers. For details about this change, see "Windows 10: Has Microsoft cleaned up its update mess? (Spoiler: no)")

Because of the enormous number of machines that receive Windows updates, Microsoft "throttles" update delivery to manage the load on its servers. As a result, it may take weeks or even months for a feature update to roll out to all of the hundreds of millions of devices in each servicing channel.

Quality updates are delivered at the same time to all supported branches. These cumulative updates arrive on the second Tuesday of each month, or Patch Tuesday, as it's widely known. (Microsoft officials refers to this day as Update Tuesday.)

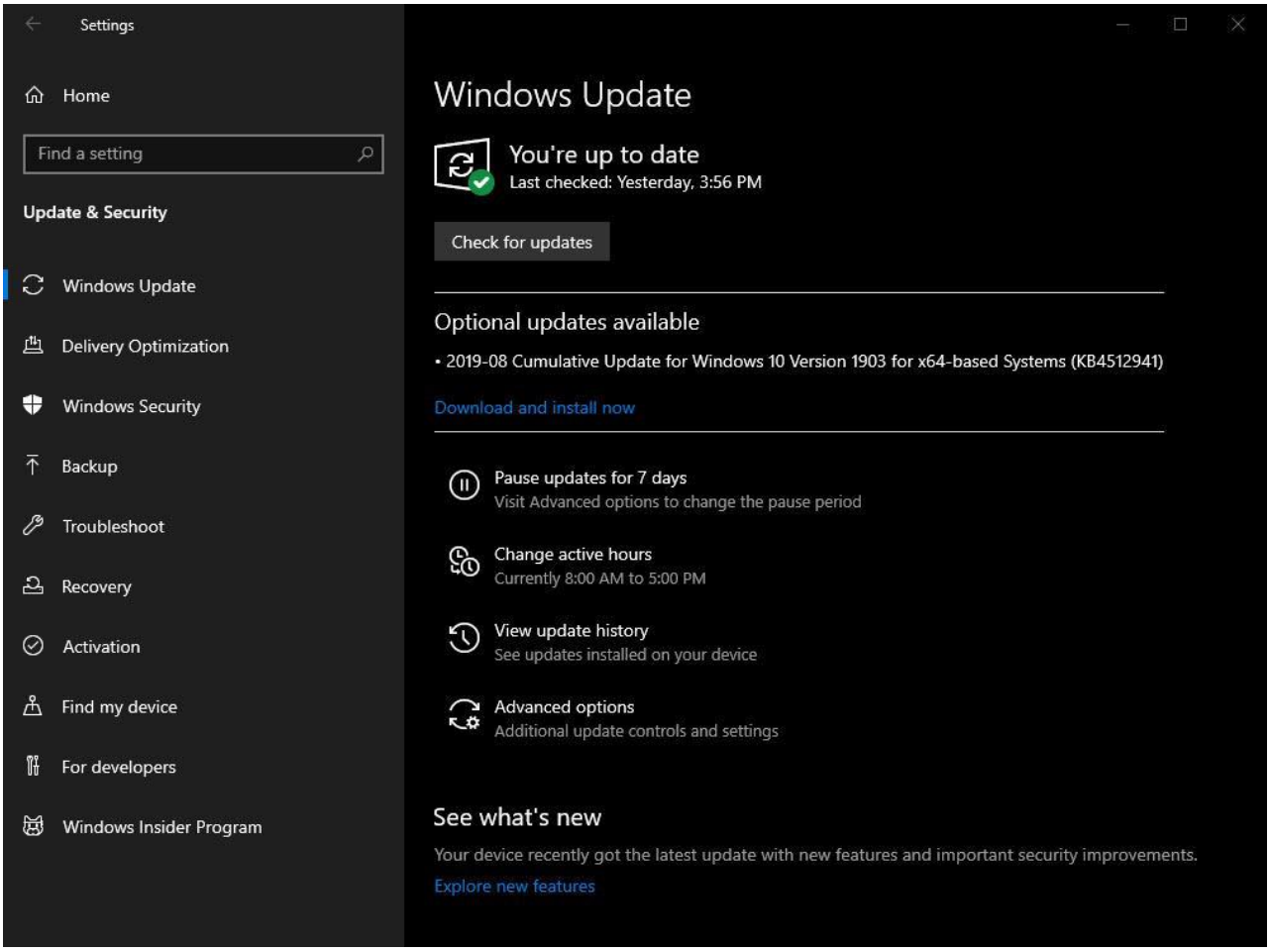
Microsoft may deliver additional updates throughout the month, including cumulative updates and servicing stack updates. So-called out-of-band patches to address critical security issues may appear at any time, generally in response to reports that a Windows flaw is being actively exploited.

WHY ARE SOME CUMULATIVE UPDATES LISTED AS OPTIONAL?

As noted earlier, Microsoft releases cumulative updates on the second Tuesday of each month. This is called the "B" release. During the third and fourth week of each month, you might see "C" and "D" releases. These cumulative updates represent previews of the following month's "B" release, and they contain only non-security fixes.

According to Microsoft, the "C" and "D" releases are "intended to provide visibility and testing" of those fixes for IT pros and enterprise administrators.

These preview releases are not installed automatically. They are visible only if you go to the Windows Update page in Settings and manually check for updates. The only way to install one of these optional updates is to click the Download And Install Now link below its entry, as shown here:



(*continued from Page 10)*

This optional cumulative update is a preview of the following month's Patch Tuesday update.

If you leave the Windows Update page without installing that update, nothing happens. The optional update disappears the following month, when it's replaced by the regular Patch Tuesday update.

HOW CAN I TELL WHICH UPDATES ARE INSTALLED?

See the list under Settings > Update & Security > Windows Update > View Installed Update History. The list is divided into three groups: Quality Updates, Driver Updates, and Other Updates. Click the entry for any update to see further details about that update, if they're available.

HOW DO I KNOW WHETHER MY SYSTEM IS UP TO DATE?

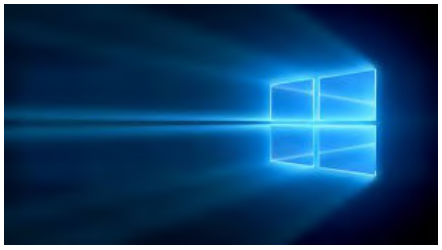
Follow this link for instructions on how to identify the build installed on your device and compare it to the master list of Windows 10 updates:

Windows 10 tip: Find and decode secret version details

To review an up-to-the-minute list of updates for all currently supported Windows 10 versions, see the official Windows 10 Update History page.

WHEN DOES WINDOWS 10 INSTALL UPDATES?

Windows 10 downloads cumulative updates in the background and installs them automatically. As noted earlier, optional updates released in the "C" and "D" weeks are not installed automatically. In addition, as of version 1903, feature updates are also not installed automatically unless the current device is approaching its end-of-support date.



Using options on the Windows Update page in Settings, you can specify Active Hours (a block of up to 18 continuous hours) when you don't want to be interrupted by these installations. In theory, that prevents a large update from interfering with your workday activities, although the strategy fails if you shut your device down at the end of the day and don't restart until the next day.

Windows 10 offers additional notification options as well as the option to choose a specific time (during your lunch break, for example) when updates will be installed.

CAN I DELAY THE INSTALLATION OF UPDATES?

As of version 1903, Windows 10 no longer installs feature updates automatically. Instead, as with the optional cumulative updates delivered in the "C" and "D" weeks, the update is listed as available in Windows Update, but you have to click Download And Install to kick off the installation. This change affects all editions, including Windows 10 Home.

If you choose not to click that link, Windows 10 will respect your decision, but not indefinitely. For retail editions of Windows (Home and Pro), each version is supported for 18 months from its initial release date. When you approach the end of that period, Windows Update will notify you that it plan to install an upgrade to the current version; you can choose the installation time within a narrow range of dates, but you can't delay the installation indefinitely.

If you're running a version of Windows 10 Home earlier than version 1903, there is no supported way to delay the installation of cumulative updates, and when a feature update is available, it will install in the next window outside Active Hours. You can try various workarounds, such as shutting off the Windows Update service or setting your network connection as metered, but these only briefly postpone the inevitable.

As of version 1903, all publicly released (non-Insider) editions of Windows 10 allow users to pause all updates. The option to pause for 7 days is available on the main Windows Update page in all editions. In business editions (Pro, Enterprise, Education), you can use the Advanced Options button to choose a specific date up to 35 days in the future. For full details about this feature, see **"Windows 10 tip: When you should (and shouldn't) pause updates."**

(continued on Page 12)

(continued from Page 11)

In Pro, Enterprise, and Education editions, you can defer feature updates for up to 365 days after their initial release. In addition, you can defer quality updates, including the monthly Patch Tuesday fixes, by up to 30 days.

These deferrals use the Windows Update for Business feature set. For full instructions on how to use Windows Update for Business, see **"Windows 10 update: The complete guide for businesses of every size."**

After you reach the maximum deferral period for each type of update, Windows 10 installs it automatically. No further deferrals are permitted.

CAN I UNINSTALL A DRIVER DELIVERED THROUGH WINDOWS UPDATE?

Yes. Follow these instructions to remove the driver and prevent it from being installed again:

Windows 10 tip: Hide unwanted drivers in Windows Update

To see the original article which contains more useful tips and FAQ's, go to:

https://www.zdnet.com/article/faq-how-to-manage-windows-10-updates/

Permission to print granted by the author

SDS Note: Still working with an old version of Windows and never got around to installing the free Windows 10 from a couple of years ago? Author Ed Bott of ZDNET has another article that will help you remedy that!

https://www.zdnet.com/article/heres-how-you-can-still-get-a-free-windows-10-upgrade/

ADANews Ransomware, Phishing Attacks Target Dentists

By Mary Beth Versaci August 30, 2019

Two recent incidents serve as reminders that ransomware and phishing attacks can affect dentists.

Hundreds of dental practices were impacted Aug. 26 by a ransomware attack against DDS Safe, a data backup system provided by a subsidiary of the Wisconsin Dental Association, and PerCSoft, a technology provider in the dental industry.

In a message to Wisconsin Dental Association members Aug. 30, Executive Director Mark Paget said the Wisconsin Dental Association Insurance and Services Corp. and PerCSoft were investigating the scope of the attack with the FBI's Cyber Crimes Task Force to determine next steps.

As of Sept. 5, PerCSoft was continuing to put clients back online, with the goal of returning everyone to full operations as quickly as possible, corporation President Mara Roberts said in an email to DDS Safe customers.

The corporation and PerCSoft also were working with a national, independent forensic team to investigate the incident, ensure it was contained and prevent future attacks, Ms. Roberts said.

Ransomware is a type of malware that denies access to a computer system or data until a ransom is paid. Law enforcement does not recommend paying a ransom, but it is ultimately up to businesses to decide if the risks and costs of paying are worth the possibility of getting their files back, according to the Federal Trade Commission.

DDS Safe facilitates secure data backups for dental practice computer systems. It is provided by The Digital Dental Record, which offers IT products and services to dentists.

The investigation had not detected any type of data compromise as of Sept. 5.

"If that changes, and investigators confirm that the attack released private business and patient data vs. simply locking it, DDS Safe and PerCSoft will immediately communicate that to impacted clients and assist them in complying with the appropriate next steps," Ms. Roberts said. "The team is fully aware of the possible reporting rules and deadlines, and is working tirelessly to determine the extent of notification — if any — that may be required."

Some affected dentists may have been contacted by outside consultants wanting to sell specialized IT and identity restoration services in the wake of the incident, but Ms. Roberts urged them to exercise caution when following advice from consultants who are not familiar with the details of this incident, as well as their practices and systems.

The corporation also advised impacted dentists to contact their business insurance, cyber insurance and professional liability carriers to determine if coverage is available and start the claims process.

"We regret the frustration and difficulty this situation has caused and have devoted all resources to resolving it as quickly and completely as possible," Ms. Roberts said.

In a separate incident in late August, three American Dental Association members contacted the ADA to report they received a phishing email signed with President Jeffrey M. Cole's name that included the ADA logo in an attachment.

A phishing email disguises itself as coming from a trustworthy source in an attempt to obtain sensitive information, such as usernames and passwords, or to deploy malware by tricking the recipient into clicking on a link or opening an attachment. Dr. Cole did not send the email.

(continued on Page 14)

(continued from Page 13)

If recipients opened the attachments, clicked a link and entered their email address and password, they should change that password as soon as possible. If they use that same password for any other online account, they should change those account passwords as well.

The Federal Trade Commission recommends that phishing victims forward phishing emails to spam@uce.gov and reportphishing@apwg.org and report the incident to the commission at FTC.gov/complaint.

This phishing scam appeared to be a targeted attack to capture dentists' passwords, with no malware attached.

The ADA Center for Professional Success offers several ways member dentists can protect themselves against cyber attacks.

Steps include training staff on basic data security, backing up data regularly and keeping a copy off-site, being wary of attachments and web links included with suspicious emails, and maintaining cyber defenses such as anti-virus and anti-malware software.

To learn more, visit Success.ADA.org.

The ADA also offers a continuing education course on phishing and ransomware at ebusiness.ADA.org.

CDA introduces new online learning platform, CDA Brightbox

November 14, 2019

Dental professionals now have an easier way to obtain continuing education credits through CDA's innovative new online learning platform. CDA Brightbox lets users access all CDA online learning courses, including the audio recordings from *CDA Presents*, in one place.

With CDA Brightbox, CDA members have 180 days to complete the online learning coursework, with the ability to start and stop as needed, and members can receive their C.E. credit within 24-48 hours of course completion. The platform also offers audio recordings from CDA's biannual C.E. convention, *CDA Presents.* Members can easily download and catch up on lectures they missed and access speakers' presentations.

As part of this new member benefit, CDA members can save 50% on online learning courses and receive discounted rates on the audio recordings offered through Brightbox.

Find more information and check out current online courses at cda.org/brightbox.

50's Sock Hop!

STANISLAUS DENTAL SOCIETY
SDS
STANISLAUS
DENTAL SOCIETY
STAFF APPRECIATION '19























Shake, Rattle
& Roll

Protecting Against the Perils of Dental Patient Data Breaches

by Isaac Kohen, Oct 4th, 2019

This pattern of data breaches is very concerning for dental practices, which are charged with protecting people's most sensitive information. What can practices do to protect themselves against this growing problem?

There has been a surge in data breaches at companies from virtually every sector during the past few years. Practically every week, the news media reports new breaches that seem to be increasing in scope and severity.

This pattern is very concerning for the health-care industry, including dental practices, which are charged with protecting people's most sensitive information. With copious amounts of patient data on file, many dental offices are sitting ducks in today's perilous data landscape.

Unfortunately, this trend is getting worse, not better.

According to the Protenus 2019 Data Breach Barometer Report, "There was a small annual increase in the number of health-care data breaches, but a tripling of the number of health-care records exposed in data breaches."

© Rawpixelimages | Dreamstime.com

This presents a two-pronged problem for dental practices. First, HIPAA charges companies that are storing patients' personally identifiable information (PII) to protect this data, and in many ways it's a tangible expression of the Hippocratic oath in the digital age.

Of course, there is also an economic component. A data breach has devastating financial consequences for companies, costing them as much as 12% of their annual revenue to repair the damage. Although exact estimates vary, the average cost of a compromised health record is $380, meaning that a data breach executed at scale can quickly put a company out of business.

This is problematic for any health-care company, but it can be especially devastating to dental practices that store the same sensitive PII as large medical practices, but operate in smaller, less fortified digital environments. Fortunately, there are steps dental offices can take to protect their patients' PII and ensure HIPAA compliance.

Implement data loss prevention strategies

When it comes to data loss prevention (DLP), the best offense is a strong defense, and that requires a DLP strategy. While there are some tangible measures, such as phishing email awareness training, that can have an impact on data security, the most important solution is found in software that prevents data movement and enforces data standards throughout the practice. In this regard, dental practices have many options. Regardless of the software selection, some features need to be non-negotiable to ensure that DLP standards are upheld.

First, choose software that restricts access to PII. Every dental practice has many team members who provide patient care. However, not everyone needs (or should have) the same access to sensitive patient data. By limiting accessibility, a practice restricts the risk pool, making it less likely that data will be accidentally or maliciously misused.

At the same time, implementing software that prevents unauthorized data movement can ensure that IT administrators are notified of unusual or unapproved data movement, which can stop a data breach before it escalates in scope and severity. To put it simply, the relatively affordable price of DLP software is the most cost-effective way to prevent a practice from being the victim of a data loss event that has vast legal and financial implications.

(continued on Page 19)

(continued from Page 18)

Train employees on proper data management

Data breaches often feel like an existential crisis perpetrated exclusively by external bad actors. The reality is much more personal, meaning that data loss events are often more explainable and preventable than people believe. Human error frequently plays a central role in a data breach, and that's good news for practices wanting to protect their patients' data because proper training can mitigate this risk.

For example, *HIPAA Journal* identified a significant uptick in medical providers using personal technology to communicate patient data. The report notes, "The Department of Health and Human Services enforces HIPAA compliance via the OCR, which is issuing financial penalties for HIPAA violations and taking a particular interest in the use of mobile technologies and communication of PHI in health-care centers and between health-care providers."

There is a myriad of ways that indifference and ineptitude can create a data breach, and dental practices can actively protect this information by training employees on best practices. What's more, they can leverage their DLP software to enforce these standards. The right employee monitoring or DLP software can provide the oversight necessary to hold employees accountable for proper data management, or it can offer real-time training to build better data management habits.

Manage IT forensics to maintain a burden of proof

Unfortunately, even when practices implement their best take on cybersecurity practices, it's possible that a data loss event will still occur. Every dental practice needs a plan for accounting for that episode. With HIPAA's enforcement rule implying steep penalties for any dental practice that fails to protect patients' PII, maintaining a burden of proof through IT forensics is a critical component of any modern data protection protocol.

Therefore, implement appropriate monitoring solutions that create a burden of proof for HIPAA compliance. If a security event occurs, your practice needs to be able to determine who accessed the affected data, how the information was retrieved, and where the data went after it was accessed.

When combined with advanced features such as metadata alerts, keystroke logs, screen session recording, and history playback, your practice can quickly understand the intricacies of the event. This can help avoid HIPAA fines while creating a framework for improving best practices.

Conclusion

Dental practices have many reasons to reevaluate their cybersecurity posture, especially when it comes to protecting their patient data. There is no indication that the digital landscape is becoming any more secure, so the impetus is on dental practices to take the steps necessary to ensure that their data integrity standards can meet the moment.

Providing excellent patient care has to include protecting patient data, and by implementing an employee monitoring and DLP software solution, dental practices can address some of the most prescient problems that compromise their patients' PII. In doing so, they protect themselves from the legal and financial consequences of a data breach.

Isaac Kohen is the Founder and Chief Technology Officer of Teramind, a leading, global provider of employee monitoring, insider threat detection, and data loss prevention solutions.

Reprinted with permission of DentistryIQ

The Joy of Special Needs Dentistry -
What they didn't teach you in dental school
with Dr. Allen Wong

Stanislaus Dental Foundation
Annual Membership Meeting
Keys to Lawsuit Prevention, Dental License Protection and Tax Savings
with Natalyn Lewis

Condolences

Patti Santini
12/18/54—9/10/19

Long time Executive Director
of the Stanislaus Dental Society

Dwight Klump, DDS
7/4/38—7/21/19

Retired member of the
Stanislaus Dental Society

ADANews Cybersecurity starts with training dental teams

by David Burger, August 28, 2017

Faribault, Minn. — In 2015, Dr. Lloyd Wallin's dental office was victimized twice in one month by hackers using ransomware — a type of malicious software that threatens to publish the victim's data or block access to it unless a ransom is paid.

Dr. Wallin

Dr. Rubinstein

Dr. Aschheim

"It happened out of the blue," said Dr. Wallin, now a semi-retired dentist in Faribault, Minnesota. "It hit us pretty hard."

In the wake of the attacks, Dr. Wallin decided to train his staff on data security. Since those two attacks, his office's computers haven't been hacked.

Dr. Wallin's training of his staff was exactly what he should have done, based on a July news release by the U.S. Department of Health and Human Services' Office for Civil Rights. The release encourages all health care providers to train their staffs on the importance of safeguarding the privacy and security of patients' protected health information in the face of cyberattacks such as ransomware.

The Office for Civil Rights said that there has been a 10 percent increase over the past two years in the number of providers and health plans that have had instances of security-related Health Insurance Portability and Accountability Act violations or cybersecurity attacks related to protected health information.

The release continues: "This increase in HIPAA violations includes breaches due to ransomware events … and other cyberattacks which could have been prevented by an informed workforce trained to detect and properly respond to them. Training on data security for workforce is not only essential for protecting an organization against cyberattacks, it is also required by the HIPAA Security Rule.

"The security rule specifically requires covered entities and business associates to 'implement a security awareness and training program for all members of its work-force.' Note the emphasis on all members of the workforce, because all workforce members can either be guardians of the entity's protected health information or can, knowingly or unknowingly, be the cause of HIPAA violations or data breaches."

The Office of Civil Rights release includes recommendations on what health providers should consider:

- How often to train workforce members on security issues. Many entities have determined that biannual training and monthly security updates are necessary, given their risk analyses.
- Using security updates and reminders to quickly communicate new and emerging threats.
  What type of training to provide, whether it be computer-based, classroom training, monthly newsletters, posters, email alerts and team discussions. The Office of Civil Rights offers training resources at hhs.gov.
- How to document training.

Drs. Mitchell Rubinstein, Kenneth Aschheim and Bijan Anvar are members of the New York State Dental Association who regularly provide training to dental societies, dentists and dental teams on protecting their computers from a data breach and how to meet the HIPAA security requirements.

The three dentists had basic recommendations on how dentists and their teams can help remain safe and protected from cyberattacks.

Dr. Rubinstein said that unlike large corporations, dental offices generally don't have an IT department to help dental teams protect themselves. "But we have to follow the same regulations."

(continued on Page 23)

(continued from Page 22)

He said that computers in the office should only be used for dentistry-related matters, and that team members should have individual passwords for using workstations.

"The most important thing is to do a risk assessment," said Dr. Aschheim. "Most people have no clue what that means."

"The one thing I stress is that staff is included in my lectures," said Dr. Anvar. "It's very important to get the entire team involved and trained." He recommended that aside from computers that contain protected health information, dental offices should have a computer that is used only for email, since email users sometimes click on links they shouldn't be clicking on. Encrypting data is also important, he said. "If the data is stolen, at least it will not be accessible."

Data breaches are not only devastating, but also costly.

"These HIPAA fines are serious fines," Dr. Anvar added.

"Nobody is immune," said Dr. Aschheim. "It's unrealistic to believe you're bulletproof."

To help dentists implement a step-by-step HIPAA compliance program, the ADA offers the ADA Complete HIPAA Compliance Kit (J598). Readers can save 15 percent on the HIPAA kit and all ADA Catalog products with promo code 17143 until Nov. 17. To order, visit ADACatalog.org or call 1-800-947-4746.

ADA 2017 – America's Dental Meeting will host a course led by Drs. Aschheim, Rubinstein and Craig Ratner, HIPAA Security Compliance: Protecting Your Practice and Your Patients (8107). Created in partnership with the ADA Council on Dental Practice, this half-day course is designed as a practical guide for dentists and their team to protect patients' electronic protected health information and comply with HIPAA security regulations. Based on standards and guidelines developed by the ADA, this course aims to provide practical, common-sense, realistic, step-by-step guidance, with an accompanying workbook, to help dental teams comply with complex regulations and avoid unwanted fines. Registration is open at ADA.org/meeting for the annual meeting in Atlanta Oct. 19-23.

The ADA will be hosting a free webinar on ransomware Wednesday, Sept. 20, at noon Central Daylight Time. Presented by ADA staff, the webinar will feature ways in how dental teams can decrease the likelihood of having their practices be attacked through ransomware and/or phishing and the HIPAA implications of security breaches. One hour of continuing education credit will be available. The registration link is https://cc.readytalk.com/r/xf56tz1str6w&eom.

For more information on how dentists can protect their practices, visit the Center for Professional Success at Success.ADA.org and search for "Tips to Safeguard Your Practice from Computer Hackers."

Burger D. Cybersecurity starts with training dental teams. ADA News. Published online August 28, 2017 at https://www.ada.org/en/publications/ada-news/2017-archive/august/cybersecurity-starts-with-training-dental-teams.

Pssst!....

It's time to renew!

Get your CDA membership set for 2020. Pay your dues and sign up for autopay by December 31 to receive a $10 Starbucks® gift card from CDA!

Giving from the……

Dr. Elizabeth Demichelis, representing Modesto Sunrise Rotary, survived going "Over the Edge" to help raise funds for Community Hospice.

Our crew is volunteering today at the 4th Annual Homeless Veterans Stand Down @ Graceda Park. Dr. Acree and Team will be providing much needed dental services to our homeless vets. Go Team!

All pink at Fletcher Dentistry today! Love. Hope. Aware #breastcancerawareness

Trudi and Dr. Andy Fletcher

Dr. Fletcher's Dental Team

SDS ED and Modesto 500 Lions Club member Robin Brown and her club provided needed items and filled back-packs for the Veterans Stand Down.

Working the Hope Dental Van today with my good friend, Dr. Corey Acree

Drs. Andy Fletcher and Corey Acree

Salvation Army's Red Kettle Kickoff—Raised $209k!

Mary Ann Sanders, Dr. Elizabeth Demichelis and mom Irma

Dr. Bruce Valentine

Drs. Brett Springer and Jake Barber

Final EPA rule prohibits 'sewering' of pharmaceutical hazardous waste

Reprinted with permission from California Dental Association

Health care facilities that produce pharmaceutical hazardous waste are required to properly manage the disposal of that waste according to the Environmental Protection Agency. Among other provisions, the EPA's finalized rule issued in July prohibits facilities from pouring pharmaceutical hazardous waste down sink drains or toilets, a practice known as "sewering."

Although the rule will have the greatest impact on hospitals, pharmaceutical retail outlets, long-term care facilities and reverse distributors, dental providers in some states will also need to take steps to comply with the no-sewering requirement by the Aug. 21 effective date.

Dentists in California will need to take little to no action to comply with the EPA rule. California dentists currently comply with the California Medical Waste Management Act of 1995, which requires that nonhazardous pharmaceutical waste be disposed or managed as regulated medical waste. The California Department of Public Health does not anticipate any changes to the act as a result of the EPA rule.

Some California counties, including Sacramento and Contra Costa, already prohibit health care providers from sewering hazardous waste pharmaceuticals. The EPA, as part of the new rule, discourages sewering of even nonhazardous waste pharmaceuticals as a best management practice.

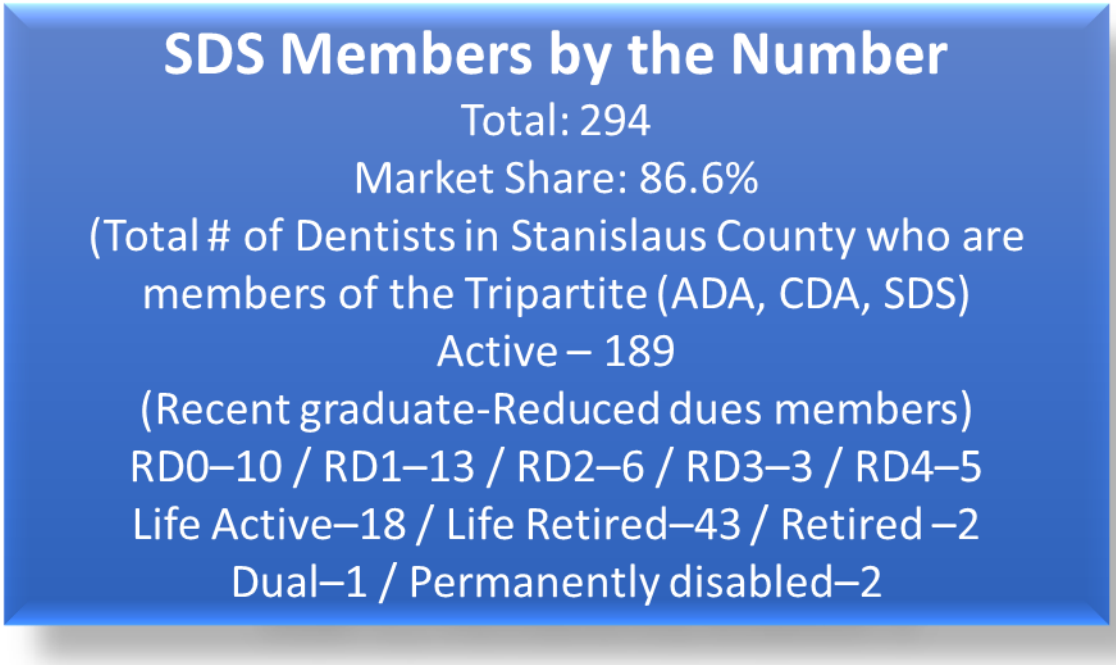
The California Medical Waste Management Act states that pharmaceutical waste:

- May not be combined in a container with other types of medical waste (sharps and biohazardous).
- Should be disposed through a registered medical waste hauler or through a USPS-approved mail-back program.
- Must be disposed within 90 days of the container becoming full or, at minimum, once annually.

Composites, bonding agents, sealants, resins and other dental devices are not considered pharmaceuticals under California's definition.

By prohibiting sewering, the final rule titled "Management Standards for Hazardous Waste Pharmaceuticals and Amendment to the P075 Listing for Nicotine" is expected to "reduce the amount of hazardous waste pharmaceuticals entering our waterways by 1,644 to 2,300 tons on an annual basis," according to the EPA.

The rule can be viewed at www.epa.gov/hwgenerators.



Why Dental Website Security is Vital to Protect You and Your Patients

by John Marks

The loss of a patient's personal information is a fundamental violation of the dentist-patient relationship. It has serious consequences for both practice and patient. This article discusses several best practices in dental website security for protecting one of your practice's most important assets.

DENTAL OFFICES HAVE THE SERIOUS OBLIGATION of ensuring that their patients' personal and financial information does not fall into the wrong hands. Theft of these details could result in a nightmare for both dentist and patient. Although security has always been a top priority for e-commerce and financial websites, a dental practice might not see itself as a natural target for cyber criminals. Health-care websites, however, are among the most common to come under threat from data thieves.

Tech-savvy patients want to feel safe when visiting a dental website, particularly when submitting sensitive information about themselves, including email addresses, patient information, and credit card details. If a data breach occurs in the transfer of information such as this, it's highly likely to break the bond of trust between dentist and patient.

When a patient settles into your dental chair, he or she is putting faith in you to care for him or her. The patient expects the same level of assurance when visiting your website. This is why dental online platforms require robust security measures to protect patients.

While the security of patients' data is crucial to reinforce the trust that a dental practice has established among its patients in demonstrating its commitment to professionalism and quality care, a data breach can also cost a dental office many hundreds of thousands of dollars in fines, civil lawsuit damages, and HIPAA violations.

Data thieves think dental websites are soft targets

There are two main reasons why cyber criminals are increasingly targeting digital records of patients. First, they view dental websites as soft targets, compared with big corporations or banks. Second, electronic health records (EHRs) of patients are extremely valuable.

As you know, a dental practice holds a vast store of information about its patients, including names and addresses, dates of birth, phone numbers, banking details, health histories and Social Security numbers.

At the beginning of 2017, Becker's Healthcare, a business and legal resource for health-care leaders, reported that data breaches were costing the US health industry $6 billion a year. (1) Protenus, specialists in protection of patients' privacy, says patients' data is a "virtual goldmine" for criminals. It says EHRs comprise a complete ID kit, enabling data thieves to steal a person's identity and commit a host of offenses. (2)

Digital identity theft enables the perpetrators to sell patients' records on the black market, acquire medical equipment or drugs they can resell, and make fraudulent insurance claims. A victim of a digital data breach faces more far-reaching problems than in the case of conventional ID fraud: if you realize someone has taken your credit card, you can simply cancel it, but when a fraudster is armed with an array of information including medical details, it can repeatedly be sold on the Dark Web—and accessed by criminals using special software to carry out untraceable transactions.

The importance of a secure dental website was underlined in 2015 when personal details of more than 150,000 patients were stolen from an Oregon dental practice after data thieves infected its computer with malware. The dental office had to offer the patients theft protection and credit monitoring services. (3)

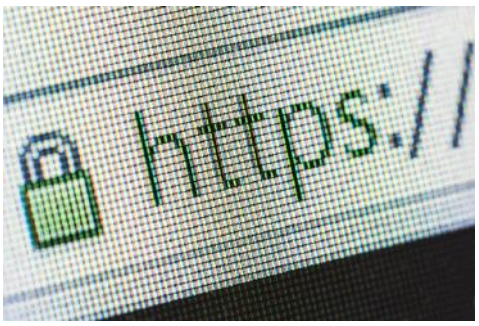
Coincidentally, while the attack on the Oregon practice was taking place, a legal specialist in dental cyber-security breaches was warning that website security was now a necessity for dental professionals. Writing for *DentistryIQ*, Stuart J. Oberman emphasized how cyber criminals were targeting small dental offices because they believed they lacked adequate online security. He said health-care organizations were involved in one-third of all data breaches, making them the single biggest victim of data breaching.

(continued on Page 27)

(continued from Page 26)

EHRs provide a versatile haul for criminals, typically worth ten times more than financial information on its own, because stolen EHRs can be bundled up in different packages that attract high levels of attention from predators scouring the Dark Web for sensitive information they can sell on an ongoing basis.

How can my practice's website be made secure?



Website security typically comes in the form of a Secure Sockets Layer (SSL) or Transport Layer Security (TLS). SSL came onto the scene in 1995, launched by the now-defunct Netscape browser, followed by TLS in 1999. These technologies establish a coded connection between a browser and a web server, while the intricacies of the complex process remain concealed from users. SSL creates two cryptographic structures—a public key and a private key—that enable a web server to establish a coded link between the website and the patient's web browser. SSL cannot stop hackers who attack computers and servers directly, so the server itself requires securities in place and the computer should have robust antivirus software.

You can tell whether a website is secure if its URL is preceded by "Secure | https." HTTPS stands for Hypertext Transfer Protocol Secure. It protects information being sent from a computer to the site it's connected to by encrypting all communications between your browser and the website. This encryption turns data into a secret code, and is the best method of providing security of information. To view the original file requires a key or password. Unencrypted data is known as plain text; encrypted data is called cipher text. Information sent to the destination server stays encoded until it is received, foiling anyone trying to intercept the data en route in so-called "man-in-the-middle" attacks.

Adequate levels of security for a dental website are required by law if the practice is considered a "covered entity"—that is, one involved in electronic transmissions of patients' information. Under the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA), overseen by the US Department of Health and Human Services, safeguards are necessary to ensure the security and integrity of health information submitted online. The Department of Health and Human Services says 21 million health records have been compromised since September 2009, and the Department's Office for Civil Rights is now conducting random audits of relevant websites, with fines averaging $1.1 million. (1) The American Dental Association describes secure encryption as an "excellent" method of safeguarding information that patients send to practices electronically.

Benefits of a secure online dental platform

Besides being a legal requirement in many cases, a secure dental website can bring many benefits to a practice.

Having a secure website can generate more patients. When a prospective patient visiting your online platform gets the reassurance of security certification, they know they will be safe when making an electronic appointment request. If your site does not display security verification, a potential patient is likely to look elsewhere for treatment.

Another way a secure dental website helps to attract new patients is that it improves search engine rankings. Google, the largest search engine in the world, boosts websites that protect the user's information. Although this measure does not currently have a huge impact on search engine results pages, it is expected to gain momentum over time, which could see any unsecured dental websites plunging down the rankings into obscurity. If patients use Google Chrome, a potentially unsafe website will show a lock with a red "X" over it. People are far more likely to stay on sites that display a green lock and an "https" address instead of just "http".

If an online appointment request form contains a description of symptoms of the problem, HIPPA deems this as Protected Health Information (PHI) that requires rigorous data security standards.

(continued on Page 28)

(continued from Page 27)

Maintaining trust by keeping your patients safe

The web comprises a complex matrix of interactions, with information of all sorts traversing across numerous networks and servers before arriving at its final destination. Any one of these systems can be hijacked by data thieves if this information is not properly protected during its journey.

A dental practice holds an enormous amount of information about its patients, including banking details and health histories, and theft of this data could have devastating consequences for both practice and patients. Trust is a crucial component in the dentist-patient relationship, and website security is essential to maintain that confidence by protecting them from cyber criminals.

Understanding the importance of website security enables dental offices to maintain the same degree of trust their patients place in them online as they have when they visit their practice for treatment. A secure site also guarantees you won't fall foul of the law.

Editor's note: This article first appeared in the *Apex360* e-newsletter. Apex360 is a *DentistryIQ* partner publication for dental practitioners and members of the dental industry. Its goal is to provide timely dental information and present it in meaningful context, empowering those in the dental space to make better business decisions. Subscribe to the *Apex360* e-newsletter here.

John Marks is the chief operations officer for DentalROI, a digital dental marketing company with over 20 years' experience in creating secure dental websites. He is a pioneer when it comes to online security development for dental websites. For more information, email him at john@dentalroi.com or visit www.dentalroi.com.

References

1. Dietsche E. Healthcare breaches cost $6.2B annually. Becker's Health IT & CIO Review website. http://www.beckershospitalreview.com/healthcare-information-technology/healthcare-breaches-cost-6-2b-annually.html. Published January 19, 2017. Accessed July 2017.
2. A Virtual Goldmine: Why Criminals Target Patient Data (Part 2). Protenus website. https://www.protenus.com/blog/a-virtual-goldmine-why-criminals-target-patient-data-part-2. Published February 15, 2017. Accessed July 2017.
3. Greenberg A. More than 150K patients impacted in Advantage Dental breach. SC Media website. https://www.scmagazine.com/more-than-150k-patients-impacted-in-advantage-dental-breach/article/535820/. Accessed July 2017.

Robin's Remarkably Brief Remarks

SDS Executive Director

The theme of this publication shows you that we are looking out for you and I hope you feel that while you contemplate renewing your dues for 2020. The SDS board and I always have members needs as our first concern and we are here for you if you need practice assistance. We want your practice to thrive and all we ask in return is your involvement in our activities, whether it be general membership meetings, social events, continuing education for you and your dental team, or service on a committee or perhaps eventually...the board.

Heads up! CDA is moving towards having members renew by EDP (electronic dues payment) by 2021. In addition to making your life easier by having your dues automatically come out of your checking account monthly (better than paying the entire amount all at once!) it make MY life easier by not having to chase down members for three months that haven't remembered to pay theirs yet; a process that literally takes many hours! Every year your membership would automatically renew for the subsequent year unless you move out of state which means no repeat emails from CDA reminding you either. Whew! See how much easier life can be?!

That's what we're all about here at SDS; making your practice life easier. And for that, I get to work with...

...SDS members (and team) who preserve the dental health of the earth's population, one patient at a time!

May the holiday season bring you happy times with family and friend, warmth, and love. Happy Holidays!

Online convenience + responsive service = stress-free supply shopping

The Dentists Supply Company continues to deliver big benefits to members of organized dentistry. With 20% average savings compared to MSRP*, shopper savings on dental supplies have already added up to more than $7 million.* In addition to controlling their overhead costs, practices of every size are streamlining and saving time by shopping tdsc.com.

Consistent supply pricing, 24/7 online convenience and responsive customer service have helped make the purchasing process quick and stress-free.

In shopping tdsc.com for his New York-based practice, Payam Goudarzi, DDS, discovered better pricing on almost all items compared to what he had been paying competitors. “The items were received at my office in about three days, and I have found customer support very helpful,” he said.

The Virginia-based general and cosmetic practice of Cindy Southern, DDS, only began shopping tdsc.com in May, but has already seen hundreds of dollars in savings on each order. The TDSC team helped her assistant set up a personalized list of the products her office frequently uses, and ordering is now fast and simple.

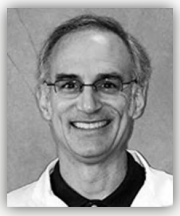
“Customer service has been fantastic!” Dr. Southern shared. “To date, we have only purchased items that match exactly what we were purchasing elsewhere. I plan on expanding our items to comparable products in the next couple of months. I would recommend this to anyone who wants to save on their cost of materials.”

The site’s satisfied shoppers have been sharing the benefits with their dental teams and peers. At the Louisiana-based practice of Matthew Ganey, DDS, office manager Tammy Arthur, compared tdsc.com’s prices to what they were paying elsewhere and was pleased to find them to be much lower. “I would suggest that all members take a few moments and check TDSC out because it was definitely worth our time!” shared Ms. Arthur.

Nava Fathi, DDS, of San Jose, California, is another one of the many shoppers who are enthusiastically spreading the word. “If you haven’t tried TDSC, give it a try! It’s free with your membership,” Dr. Fathi says. “You have nothing to lose.”

To discover a better way for your team to shop for dental supplies, visit **tdsc.com**.

* Savings compared to the manufacturer’s list price. Actual savings on tdsc.com may vary.



The Study of Orofacial Pain is Foundational to Unlocking Many Dental Mysteries

by John Orsi, DDS

We don't know what we don't know. Is ignorance really bliss? Those of us who have been around the block long enough have witnessed dental topics of interest come and go. Occlusion, TMD, the integration of implants, and sleep dentistry to name a few. All of these topics are important, have their place, and never go away. None of these topics developed into a specialty within dentistry, so who is best prepared to provide these services?

Around 2009, UCLA became the first University to offer an evidence-based specialty program called Orofacial Pain and Sleep Medicine as a new discipline within dentistry. This new discipline systematically brings together medicine and dentistry in order to stop the finger pointing in medicine and dentistry in the treatment of patients who have any head and neck pain. CODA, the organization that accredits dental schools recognizes over a dozen of these programs in the United States, yet ADA still can't decide if this should be a specialty within dentistry or medicine.

Politics aside, why wait to learn more about this discipline? Patients benefit from our improved knowledge base and this discipline brings new light to all four of the above-mentioned topics. When it comes to occlusion, there will always be a great divide between those who have a different agenda. If all you have is a hammer, everything looks like a nail. Some may say "occlusion is not that important" and claim it is better to use an articulator that recreates a system where the TM joint is an approximation of a hinge at the atlas and axis of the neck. The reality is there is a different knowledge base required when focusing on the treatment of pain as opposed to the rehabilitation of mastication. Although it may be true and it seems like heresy to say: In the treatment of TMD pain, occlusion is not the most important risk factor. That does not have the same meaning as, "Occlusion is not that important." Teeth still need to function properly and many times the way the teeth look matter to the patient. But wouldn't it be nice to get a patient out of TMD pain quickly and efficiently first before rebuilding their mouth?

Chronic and acute pain are different animals. By definition chronic pain begins with acute pain. The key is to keep the acute pain from becoming chronic. One of the best ways to do this is to understand both. Our world in dental school focused on the diagnosis and treatment of acute pain. As dentists, we are the trained medical specialists of acute pain in the mouth. However, our dental school training left us with a blind spot to chronic pain. Those patients that don't respond to the treatment we were trained in are then perceived as crazy. Don't get me wrong. There are patients that are crazy that also have pain, but most chronic pain patients really do have legitimate reasons for their pain that can be managed.

When pain after surgery occurs, be it from implant placement, extractions, endodontics, or restorative dentistry, why does this happen? Why is it more intense with some patients? Why does it linger longer in other patients? Why does it sometimes become chronic? These are all fundamental questions answered in the study of orofacial pain. Wouldn't it be nice to recognize the susceptible patient and pre-emptively prevent a bad experience?

And then there is sleep dentistry. As soon as someone recognizes a "profit center" in the practice of dentistry, weekend courses materialize overnight to fast track its incorporation. To this I say two things; consider the source, and do no harm. What medical screening was performed as a diagnosis before treatment? Making an oral appliance prior to a diagnosis is like putting the cart before the horse. Sounds like we are revisiting that saying again…if all you have is a hammer everyone looks like a nail. If you treat snoring by using an oral appliance in a patient with moderate to severe sleep apnea, you might stop their snoring but could actually be killing them slowly by avoiding definitive resolution of the apnea. Although sleep apnea is the most common type of sleep breathing disorder, it is only one of a long list of other conditions it is important to rule out before considering an oral appliance, a complex restorative treatment, or pain management plan.

Last month the Stanislaus Dental Society offered an introductory evening and all-day course on orofacial pain. It was a pleasure to help bring to light some of the things you may not have known. I hope the review of a some of the concepts presented are implemented like the cranial nerve exam that could help identify a brain tumor and simple forms to look at the possibility that anxiety, headaches, or a sleep disorder could be an obstacle to a positive patient outcome whether it is for restorative dentistry or pain management. I encourage you all to keep taking advantage of opportunities to learn more about this area of study.

the Boo Crew


TRICK OR TREAT
BRUSH
FLOSS
FLEEK


KIM 1
KIM 2


Halloween
CANDY
BUY BACK
Swanberg & Sceville Dental Office
All candy will be sent to our troops overseas for a special treat!

Ad

Rotary Club of ModestoFLEX

New "Flexible" Rotary Club chartered in Modesto

Fewer meetings, more family involvement emphasized

The civic scene in Modesto may have changed forever. While service club memberships have suffered from a downward trend across the globe for the past two decades, 41 members are active and already beating the odds. Sponsored by Rotary Club of Ceres, the new Rotary Club of ModestoFLEX chartered on January 9, 2019 with 30 charter members.

"We're thrilled to have officially chartered earlier this year," said Eugene Awuah who is serving as the club's first President and leads Rotary membership growth efforts in the Central Valley and Mother Lode. "What was once a dream is now reality. We are living the dream and want to share this flexible and fun experience with you and your family."

Most traditional Rotary clubs world-wide hold weekly adults-only meetings during business hours with firm attendance requirements and mandated meals. ModestoFLEX marries the same Rotary principles and benefits with a more flexible and less costly format. "We keep the cost and time commitment down to appeal to families who may have hesitated becoming Rotarians in the past," says Public Image Chair Michael Gaffney. "Achieving work life-balance is a real problem. Setting aside time to give back to the community is challenging for many families. The FLEX concept is proving to be the solution. My wife Victoria and I each hold a leadership role on the board and take our four-year-old son Connor to the meetings. Instilling Rotary's solid values and morals in him is very important to us."

The club's enthusiastic, diverse, and growing membership has quickly fostered a very positive club culture that promotes a warm, welcoming, and inclusive environment for all who value family, life-long friendships, and a hands-on approach to Rotary service. "I've been searching for a place to develop my leadership skills while pursuing my passion for financial literacy. ModestoFLEX provides me with both," says young business professional Cecilia Rosales who is proud to be the club's President-Elect.

An array of affordable membership levels is available including: Individual, Single Family, Couples Family, Small Business, Corporate, and Young Business Professionals. "The FLEX concept provides me with a vehicle to do something about homelessness in our community, an issue that needs our immediate attention," says big-hearted but time-challenged local business owner Dory Tucker, who recently launched The Hopeful Garden Project that focuses on homeless mitigation.

ModestoFLEX meets on the first Wednesday of the month from 6:00 to 7:30 p.m. at rotating locations including member's place of work. The second meeting is also flexible with dates and times agreed to by members ahead of time based on their work and family schedules.

To learn more about the Rotary Club of ModestoFLEX or attend an upcoming event, please contact Michael Loschke at 209-988-2000 or visit www.facebook.com/modestoflexrotary.

Holiday Member Mixer

Do You Pay Your Team Members on a Salary Basis? The Rules are Changing!

by Kara Kelley

For the first time in over a decade, the U.S. Department of Labor has issued a final ruling on an increase to the salary threshold for exempt employees. Starting on January 1, 2020, employees will need to be paid a minimum of $684 per week or $35,568 per year to meet the salary qualification for exempt status. This is an increase from the current exempt threshold of $455 per week or $23,660 per year.

What Does This Mean for Dental Employers?

If you are paying any of your employees on a salary basis you need to know whether you're paying employees as "salary exempt" or "salary non-exempt" – and if you're in compliance with federal rules.

To understand this, you need to separate the payment method from the classification. Salary and hourly are payment methods. Exempt and non-exempt are employee classifications. More specifically, the latter categorizes employees by determining whether they are exempt from the Fair Labor Standards Act requiring non-exempt employees to be paid minimum wage and overtime pay. You are not required to pay overtime to exempt employees so long as they are paid the same amount of salary each week.

Exempt vs. Non-Exempt Employees

Most employees in a dental practice are non-exempt because they do not meet the two standards for exemption. To consider an employee exempt from FLSA, they must be paid at least the minimum salary threshold *and* meet a duties test in at least one of the three categories: executive, administrative, or professional.

You know the new salary threshold but let me simplify the duties tests. In most cases, it's likely the only two positions in your practice that meet qualifications for exempt status are your Dental Associate (professional exemption) and your Practice Administrator (executive exemption). The PA or Office Manager can be exempt so long as they are directly managing at least two employees with the authority to hire, fire, or discipline those they supervise. The Office Manager who just makes the schedule and deals with patient complaints while still taking on the regular front desk administrative duties would not qualify as exempt.

All other employees should be considered non-exempt. In some cases, there can be exceptions made for a hygienist who has completed four years of professional study. However, their education must be obtained from an accredited college or university that was approved by the American Dental Association's Commission on Accreditation of Dental and Dental Auxiliary Educational Programs at the time of study. If your hygienist consistently works less than 40 hours per week, it's likely not worth the risk of classifying them as exempt if they do not meet the qualifications.

Pro tip – you won't have any problems classifying an employee who *could* be exempt as non-exempt; however, you could have an expensive problem if you classify an employee who *should be* non-exempt as exempt. The safer course is to consider the rest of your team as non-exempt employees, require them to track their time, and pay the overtime rate (1.5x regular hourly rate) for any hours worked over 40 in a 1-week period.

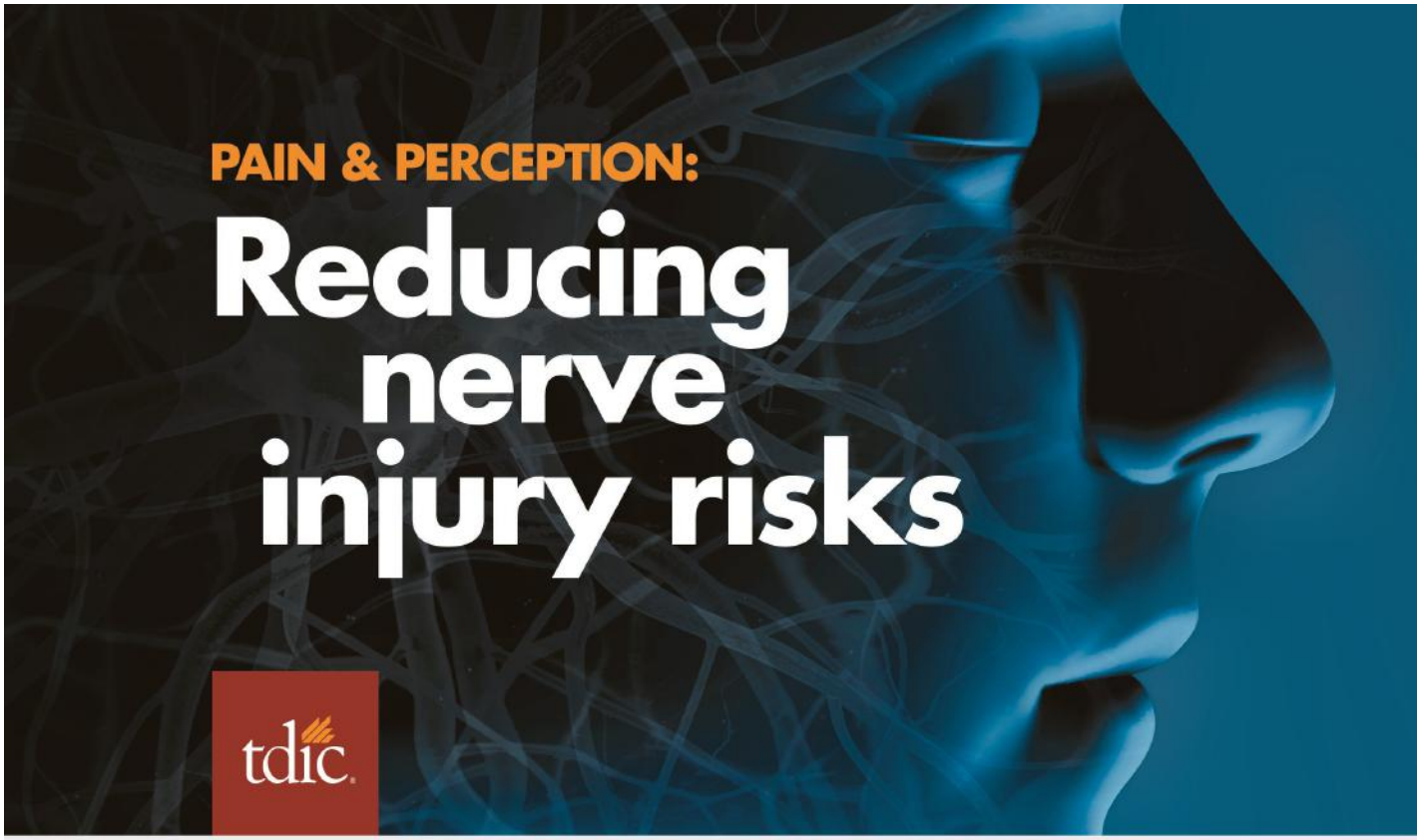
What If I Pay All My Employees A Salary?

Occasionally, an owner dentist will tell me they pay their entire team on a salary basis. Either they heard it was a good idea for employee retention or they don't want to deal with time sheets. Regardless of the reason – or whether this is a good idea, which is an entirely different article – there needs to be an understanding of the regulations surrounding employee classification.

You can have a "salary non-exempt" employee. However, because this employee does not qualify for exempt status, you should require them to track their time and will need to pay the overtime rate for any hours worked over 40 in a 1-week period. To calculate this rate, divide their weekly salary by 40, then multiply by the number of overtime hours worked and add to the base salary pay for the week overtime was earned.

It's not as complicated as it seems. Just be aware that if you have a truly exempt employee, you need to ensure they are paid the minimum salary threshold each week they work to avoid paying overtime. If you are paying a set salary to non-exempt employees, regardless of how much the salary is each week, you need to have them track their time and are required to pay them overtime (or make sure they don't work past 40 hours in any given week). Stay compliant!

Reprinted with permission from Parkhurst & Associates CPA PC 1603 Medical Pkwy, #300 Cedar Park, Texas 78613 United States (512) 582-7500



Unsure how to handle patients who are experiencing prolonged numbness following dental procedures? The Dentists Insurance Company's new Risk Management seminar is designed to build your confidence in these interactions.

Participate in the Pain & Perception seminar and learn how to:

- Institute communication protocols when multiple dentists are involved in treatment.
- Recognize the importance of complete and appropriate documentation.
- Communicate unexpected treatment outcomes to patients and know when to refer.
- Understand that informed consent is a process, not a form.

Get expert advice while earning **C.E. credits** and a **5% Professional Liability premium discount*** for two years.

Save your spot today at **tdicinsurance.com/seminars** or explore convenient eLearning options.

*TDIC policyholders who complete a seminar or eLearning option will receive a two-year, 5 percent Professional Liability premium discount effective their next policy renewal. To obtain the two-year, 5 percent Professional Liability premium discount, Arizona, California and Nevada dentists must successfully complete the seminar by April 26, 2019. Alaska, Hawaii, Illinois, Minnesota, New Jersey, North Dakota and Pennsylvania dentists must successfully complete the seminar by October 26, 2018. Any eLearning tests received after the deadline will not be eligible for the discount. Non-policyholders who complete a seminar or eLearning option and are accepted for TDIC coverage will also be eligible for this discount.

Protecting dentists. It's all we do.®

800.733.0633 | tdicinsurance.com | CA Insurance Lic. #0652783

Endorsed by the Stanislaus Dental Society

Calendar 2020

January

1	Happy New Year!! - (office closed)
7	SDS Board Meeting—6:00pm
10	BLS Renewal-9:00am-12:00pm
20	Martin Luther King Day (office closed)
24	CE-OSHA/DPA/Infection Control—8:00am-3:30pm

February

7	BLS Renewal-9:00am-12:00pm
13	General Membership Meeting-6:00pm
17	President's Day (office closed)

March

6	BLS Renewal-9:00am-12:0pm
10	SDS Board Meeting
20	CE-Pediatric Dentistry for the GP

April

3	BLS Renewal-9:00am-12:00pm
16	Shred-it Event-4:30-7:00pm

May

1	BLS Renewal-9:00am-12:00pm
12	SDS Board Meeting-6:00pm
14-16	CDA Presents-Anaheim
19	SDF Board Meeting-5:45pm
21	General Membership Meeting-6:00pm
25	Memorial Day (office closed)

June

5	BLS Renewal-9:00am-12:0pm
26	Summer Dental Symposium-8:00am-5:00pm

July

3-4	Independence Day (office closed)
7	SDS Board Meeting-6:00pm
17-18	CDA Cares—Long Beach

Welcome New Members!

Shaghayegh Bidgol, DDS
General Dentist
Suave Dental Group
3025 McHenry Ave, Modesto—527-3990
Roseman University of Health Sciences, 2018

Cheema Taranvir, DDS
General Dentist
No practice address listed
UCSF, 2019

Ryan Evans, DDS
General Dentist
Aspen Dental
3900 Sisk Rd Ste O, Modesto—857-3910
UCLA, 2017

John Farah, DDS
General Dentist
Aspen Dental
3900 Sisk Rd Ste O, Modesto—857-3910
University of Florida, 2015

Terry Fosberg, DDS
General Dentist
In practice w/ Dr. Robert Rosenbaum
2200 McHenry Ave Ste B, Modesto—526-9132
UCLA, 1973

Gerardo Malogan, DDS
General Dentist
In practice w/ Dr. Robert Rosenbaum
2200 McHenry Ave Ste B, Modesto—526-9132
UOP Arthur A. Dugoni School of Dentistry, 1994

Denis Mustedanagic, DDS
General Dentist
Western Dental
1720 E Hatch Rd, Modesto—241-5905
Case Western Reserve, 2019

Dung Nguyen, DDS
General Dentist
No practice address listed
Creighton University Boyne Sch of Dentistry, 2019

Elizabeth Reynoso Valdez, DDS
General Dentist
Trinity Dental and Implant Center
3100 E Service Rd Ste 101, Ceres—542-9921
International, 2017

Olivia Royea, DDS
General Dentist
Kids Care Dental
1840 N Olive Ave Ste 4, Turlock—668-3227
Herman Ostrow School of Dentistry of USC, 2019

Brandon Sierra, DDS
General Dentist
Quality Dentists
In practice w/ Dr. Wesley Wong
3608 Dale Rd, Modesto—577-0777
UOP Arthur A. Dugoni School of Dentistry, 2019

Shabnam Sorooshiani, DDS
General Dentist
Western Dentist
703 N Golden State Blvd, Turlock—216-4198
Nova Southeastern University, 2019

Alvaro Valencia Baez, DDS
General Dentist
No practice address listed
Mexico-Universidad De La Salle, 2017

Classifieds

- **GD Full-time assoc.**—Looking for a full-time associate general dentist in Modesto, CA for a busy, modern, multidisciplinary dental practice. We have a great staff and are looking for someone great to be a part of our team. Needs to be a team player, detail-oriented to exceptional dental work and have great communication skills. We have a lot of technology in office: CEREC, CBCT, digital charts, digital sensors, intraoral cameras, implementing CAMBRA, 3D printer, in house ortho, and Invisalign. We also place implants, make our own surgical guides, molar RCT and EXT.

  All are welcome to apply. Competitive compensation package around 25-30% collections, health benefits, 401K and many more items to discuss. Please send your resume to set up a phone interview, paxmandental@gmail.com

- **GD Modesto area**—Modesto area private practice looking for a general dentist to take care of my patients and keep my practice growing for a few years while I'm on extended leave. I have an office manager and consultant to help make your transition as easy as possible. I work normal hours 4-5 days/week. Your daily salary will be $1,000/ day or a percentage of production (whichever is higher). Please send your resume to modestodds88@gmail.com

- GD New Practice Start up!—Competitive compensation package around 25-30% collections. Office location has been determined. Contact Dr. Sefcik (801) 372-0439 for more details. If there is no answer, leave a message.

- **GD Associate Modesto**—Private practice in Modesto seeking an Associate Dentist to join our excellent team who provides exceptional dentistry. Very competitive compensation package based on experience.

  Please email your resume to 209dentist@gmail.com with the best time to contact.

- **GD Associate Modesto**—Well-established Modesto general dentistry office is looking to add another doctor to the team. The owner doctor purchased this practice 5 years ago and it is stable and growing rapidly. Presently, we average over 30 new patients a month. The office is currently open Monday through Thursday and have just recently added Fridays. This is a wonderful part-time or full-time opportunity for a doctor with a minimum of two years experience to move into a practice that is a finely-tuned machine. The salary structure is to be determined by the candidate's qualifications. Please send resume to stan@stanlent.com.

The above Classified ads are also listed on the SDS website, stanislausdental.org. SDS offers its members free advertising related to their practice including, member employment, equipment to buy or sell and practice sales or purchases. For more information, contact Robin at the SDS office, 522-6033.

Did you know?.....

In addition to posting a classified ad on the SDS website and APEX Newsletter, CDA also has a classified section where you can post jobs, dental equipment, practice sales, etc. Free to CDA members! To post or view current ads, go to….www.CDA.org/jobs