TROJAN TODAY

AUG 2022
VOLUME 25 • ISSUE 08

WWW.TROJANONLINE.COM

Five Steps toward HIPAA Compliance

The knowledge contained in the minds of staff in any dental office is immense. Dental anatomy and physiology, general health and welfare, cleaning, x-rays, prepping, billing, customer service. The list goes on. Many procedures and protocols make an office run smoothly and efficiently.

On top of everything else, it is critical to take steps to keep your digital world secure and your patients' information safeguarded. Nothing will stop business faster than malicious software that takes over your network. Someone could steal your office's financial information, protected patient health information, and log-in credentials for numerous websites.

continues on page 2

previous page

To dramatically reduce the risk of an attack, take these five steps today:

1

Ensure each user has a unique log-in.

Passwords are a pain, but they are vital. Enforce a strong 10-character minimum password policy. You are probably familiar with password requirements for most websites: upper- and lower-case letters, numbers, and a special character. And although the address of your office meets those requirements, it does not make for a secure password. Nor do such easily-guessed ones as Dental/22 and Teeth123$.

Along with the unique password, each user should only use a computer in which they have entered their unique credentials. When you are leaving your computer, lock it (Windows key + L) so no one can use the station as YOU. Logs are created that show when each person is logged into each computer and might be used to trace a leak of **PHI (Protected Health Information)**. A patient has the right to a list of those who have accessed their PHI, when it was accessed, and for what it was used.

Implement a schedule to change and update passwords during each year. Once a year at a minimum for password changes should be sufficient and not difficult for your employees. Also, make sure no passwords or any form of log-in credentials are posted or visible around the office.

2

Always call and verify when you get an email with attachments you were not expecting.

It is routine to send and receive additional documentation from patients, insurance companies, or specialty offices on a regular basis. Many offices, to reduce paper waste and clutter, have made efforts to make this additional documentation completely digital. Email and fax services will create PDFs that can be easily viewed and stored for later. This opens offices to malicious attacks through software embedded in attachments.

Follow simple rules to keep your network and patient PHI safe:

1. **If you are not expecting it,** do not open the attachment.
2. **If you do not recognize the sender,** do not open the attachment.
3. **If there are obvious grammar and spelling errors in the email,** do not open the attachment.

Take time to reach out to the sender by phone or by a separate email, to ask what was sent. Or log into your online account for that insurance company to see if messages or documents are waiting for you. Their websites are secure for the exchange of information. Email is not a secure means of sending PHI.

3

End of day security checklist

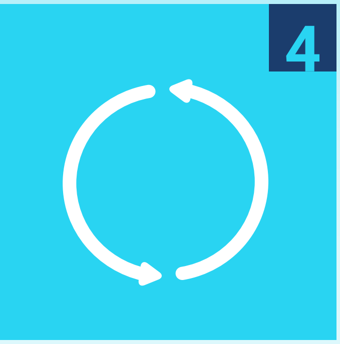
Your office can take a vital step to secure patient PHI with a simple checklist, to be completed each day. It can identify staff members who need additional training on HIPAA and provide instruction as to how to secure PHI. By using a daily checklist, you establish a history of standard office procedures for digital security which can help if there is ever a question about how your office handles sensitive information.

End of Day Checklist

- ✓ Stations are locked or shutdown.
- ✓ User IDs and Passwords are not posted near station.
- ✓ No PHI unsecured and visible at desk.
- ✓ NO PHI visible near shredder.
- ✓ Laptops and any portable equipment containing PHI are physically secured.
- ✓ Doors and windows to office are locked.

next page

previous page

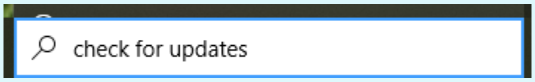


4 Keep your operating system up-to-date.

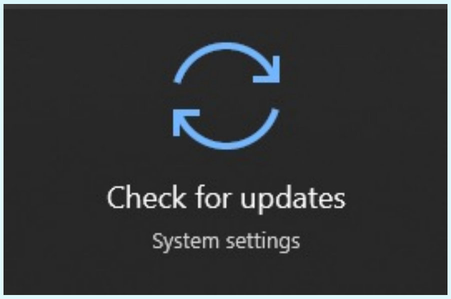
Check regularly for any updates. If you have an outside company that takes care of your computers, verify they are keeping up with the latest updates and securing your regular back-up of data.

If you are responsible for the computers, you can check for updates on a PC by simply typing “check for updates” in the search box at the bottom left of your screen.

Then click the Check for updates shortcut that appears.



check for updates



Check for updates

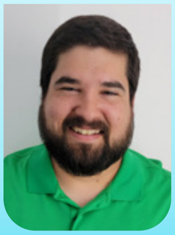
System settings

Remember to back up office data regularly. Your practice management system may have a routine for backing up the information saved inside your program. Call your support team to confirm instructions for running and securely saving the information.

5 Secure or shred any hard copies that contain PHI.

Printouts and forms from insurance companies identify the insured person so you know to which patient the correspondence refers. Notes you make when talking to an insurance company might have social security numbers, subscriber IDs, dates of birth, and descriptions of procedures on them. Do you use a hard copy form for your insurance verification? All of that is PHI and needs to be secured when you are away from your station. Turn the pages over, put them in a drawer, and be sure they are shredded when you are finished.

There are plenty of resources regarding HIPAA compliance including programs, books, seminars, and consultants. You can find a consultant or company that specializes in compliance for the dental field. If you contract with a company for your human resources, ask about employee training videos. YouTube has videos that explain HIPAA and best practices to be compliant. **Document all training:** who was there, how much time was spent, and what was the topic. You can put together a simple list for onboarding new employees and keep records of your efforts to be compliant.



__Corey Murillo__ has been Director of IT at Trojan Professional Services since 2016. He is directly responsible for Trojan attaining and maintaining EHNAC Accreditation.

FMI: *www.ehnac.org*

__Nikki Myers__ is the Marketing Coordinator for Trojan Professional Services and has been the Publishing Coordinator for __Trojan Today__ since 2018.

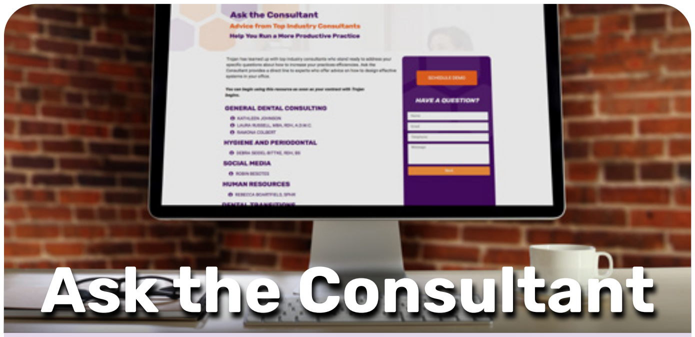
FMI: *NikkiM@trojanonline.com*

Quote-Worthy

> *“Motivation is the art of getting people to do what you want them to do because they want to do it.”*
>
> — Dwight D. Eisenhower

next page

◀ • • • previous page



Ask the Consultant

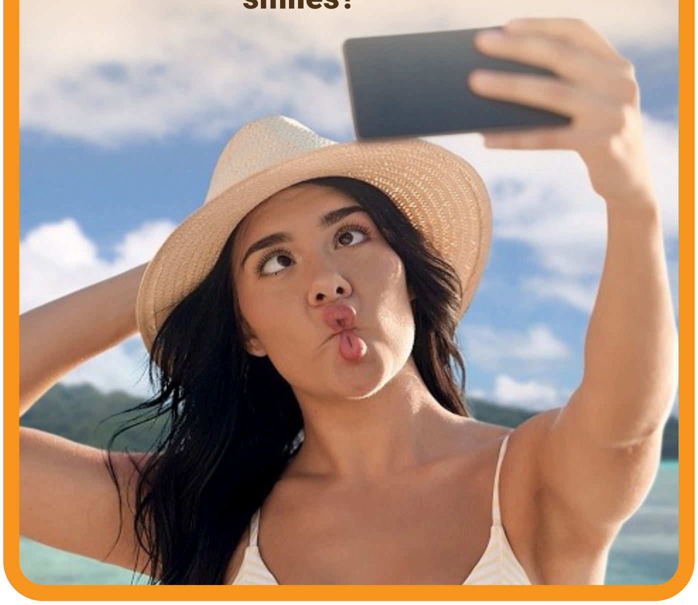
Q: A patient has a false tooth that is splinted to her other teeth. It has gotten loose, and she is getting married and wants something done. My question is: How can I bill it to the insurance company? I thought of using code *D6253*. It is a pontic, but I am not sure if that would be the right code.

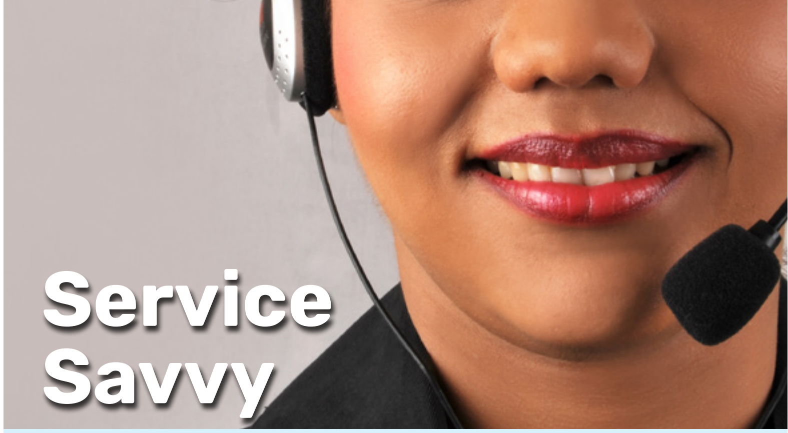
A: There's no existing code to describe this type of service so you'd use a non-specified code ***D2999***. It's very doubtful the insurance will pay for this service.

Response provided by ***Ramona Colbert***.

FUN! Fact

Did you know 48% of the reasons people give for untagging themselves in Facebook photos involve self-criticism of their smiles?



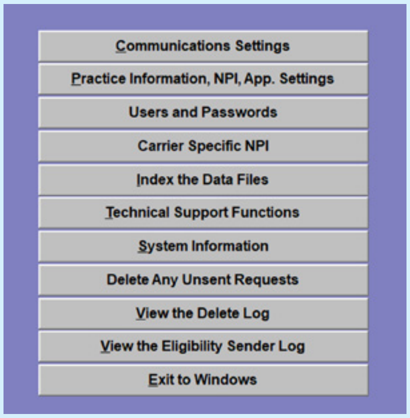


Service Savvy

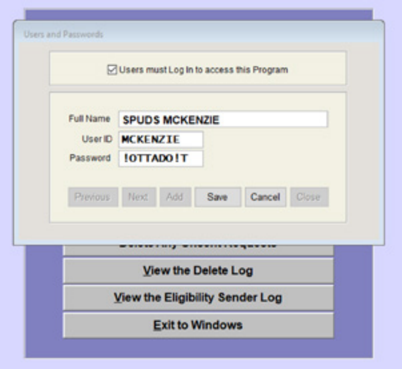
Securing the **Trojan Eligibility Request Program** with a Password

Your **Trojan Eligibility Request Program** can be secured with a password so that all patient PHI is behind one more layer of protection.

- Open the latest version of the **Trojan Eligibility Program** from your desktop.
- Go to the **Setup** tab.
- Click on **Users and Passwords**.



- Click **Add**, and check the box next to **Users must Log In to access this Program**.
- Begin adding your first user by entering **Full Name, User ID**, and unique **Password.**

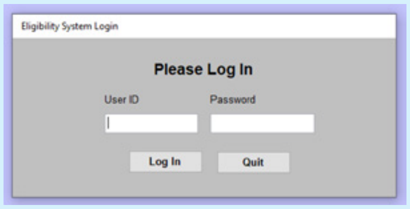


Users and Passwords

☑ Users must Log In to access this Program

Full Name SPUDS MCKENZIE
User ID MCKENZIE
Password !OTTADO!T

When you exit the program, you will need the **User ID** and unique **Password** to open it.



Eligibility System Login

Please Log In

For more information, please contact our Software Support Department at 800.451.9723, ext 1., Monday through Friday, 6 AM to 4 PM PST.

next page • • • ▶

previous page

Check it Out!

Sleep Apnea for the Front Office:
A Series of Webinars with Jan Palmer

AUGUST 16, 2022: Avoid claim denials, medical guideline standards. Pass an audit.

SEPTEMBER 13, 2022:
Coding and billing sleep appliances.

OCTOBER 4, 2022: Medicare Basics—Decisions, Decisions and Decisions

OCTOBER 11, 2022: Medicare Digging Deeper

Sign up for 1 or more. *Register Here!*

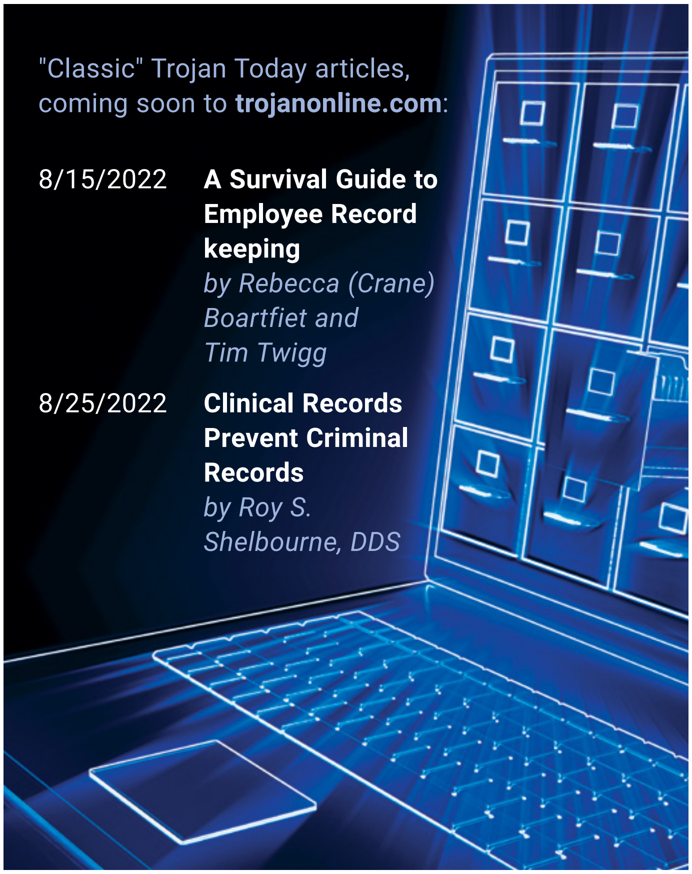
Are you a member of AADOM?
This national group for office administrators and managers hosts events throughout the year.

Dental Seminars for Dental Office Managers
AADOM Events: *dentalmanagers.com*

Christine Taxin is visiting
AADOM chapters in the East:
NE FLORIDA CHAPTER—AUGUST 18, 2022

Click here for more information.

Live Events Are Returning!
Many are listed at: www.conferenceindex.org. Search by your field or specialty.



"Classic" Trojan Today articles, coming soon to **trojanonline.com**:

8/15/2022 **A Survival Guide to Employee Record keeping**
by Rebecca (Crane) Boartfiet and Tim Twigg

8/25/2022 **Clinical Records Prevent Criminal Records**
by Roy S. Shelbourne, DDS

What Clients Say

*"You guys are great!
We have been long time customers and have NEVER been disappointed by any representative you employ."* **— Kathy**

http://bit.ly/FBTrojan

http://bit.ly/YouTubeTPSINC

http://bit.ly/TPSLinkedIn

http://bit.ly/TrojanInstagram

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

TROJAN PROFESSIONAL SERVICES

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 or staff assume 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 and with the understanding that neither the publisher, the Editor or the staff is rendering 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:** Romalyn Tilghman • **PUBLICATION COORDINATION:** Nikki Myers • **GRAPHIC DESIGN & PRODUCTION:** Moller Creative Group