

Dr. Darrell Pruitt

Questions to TDA, 6-3-10

The Texas Dental Association (TDA) staff is dedicated to providing members with excellent customer service. Part of the responsibility in fulfilling this duty is ensuring that the information provided from this office is based on facts and in accordance with applicable state and federal laws. When answering members' questions, TDA staff does not engage in speculation, hypothesizing, nor recitation of personal opinion. Information provided to members is from trusted reputable sources, and/or directly from relevant regulatory and government agencies.

Several of these questions seem to call for speculation by TDA staff and or hypothesizing, a practice, as stated above, that TDA staff does not engage in. Therefore, we have limited our responses to questions in which answers are based on fact and where relevant information can be derived from an appropriate source such as a government website. Questions and/or parts of questions marked with a bolded asterisk (*) are, in our opinion, inappropriate to answer because the prospective answers would be speculative and/or up to the discretion of individual practicing dentists. Additionally, several of these questions contain subjective terms/words, and we are unclear what you think these terms mean; for example the phrase "satisfactorily resolved." It seems that unless TDA staff shares the same understanding of such terms, any response provided to you will likely be unacceptable and encourage a circular written jostling with no clearly identifiable ending point.

- 1. - On the ADA Advocacy page, it states that eDRs will save money in dental care. Do HIT experts in the TDA agree?**

While the TDA does not currently have a policy statement on the efficacy of electronic dental records, the Association continues to monitor both federal and state developments with respect to this issue.

- 2. - Which dental records are safer, digital or paper? ***
- 3. - Do eDRs offer any benefits that are not adequately met by telephone, fax and US mail - which don't involve HIPAA? ***

HIPAA

- 4. - Why has it been so difficult for this TDA member to receive information about HIPAA from the TDA beyond non-interactive links to unhelpful government agencies and committee-approved ADA talking points?**

The TDA has engaged in several different methods to provide TDA membership information about HIPAA related issues including print, in person, and electronically. For example:

- o TDA's Council on Dental Education Trade and Ancillaries hosted the first "ADA HIPAA Compliance Meeting" at the LBJ Library at the University of Texas in Austin in 2002, followed by three additional trainings in River District, San Angelo, and Abilene in 2003.

- o Several articles regarding HIPAA have been published in the TDA Today from 2002 through 2010. The first official article regarding HIPAA was printed in September, 2002. (attachment 1)
- o There is a portion of the TDA website dedicated exclusively to HIPPA which is accessible by visiting <http://www.tda.org/displaycommon.cfm?an=1&subarticlenbr=457>

5. - **Are there plans for greater transparency in the TDA regarding government regulations? They are coming faster than the ADA lobbyists can keep up with, and will soon overwhelm dentists in Texas without warning. This month, ADA members missed the public comment period for the new HHS disclosure rule that requires dentists to notify HHS each time Protected Health Information (PHI) is included in electronic transmission of dental claims. This tedious chore will be burdensome, costly, and it will add one more regulatory obligation that an unobservant dentist can be heavily fined for “willfully neglecting” his or her responsibilities to the nation. It is time for TDA leaders to assure Texas dentists that the new, oppressive rules protecting digital information do not apply to dental claims that are mailed. ***
6. - **In the past, the TDA has actively promoted adoption of National Provider Identifier (NPI) numbers. How successful was the effort? What percent of TDA members have NPI numbers? What percent of non-TDA Texas dentists have NPI numbers?**

There is a difference between actively promoting and encouraging compliance. The TDA disagrees with the characterization that it “actively promoted” adoption of the National Provider Identifier (NPI) number. As a professional association of member dentists, the TDA encourages its members to comply with the NPI as it does with all federal and state regulations and laws.

The TDA does not collect information regarding how many members and non-members have NPI numbers. However, there are certain enumeration statistics available on the Centers for Medicare and Medicaid Services (CMS) website. The CMS’ enumeration report lists the number of individuals, organizations, and the total number of providers with an NPI number. In Texas, a total of 171,151 individuals and organizations have an NPI number. Out of the total number, 117,784 individual providers and 53,367 organizations have NPIs.

Additionally, the American Dental Association states that additional NPI data based on medical taxonomy is obtainable through CMS for a fee.

7. - **Since the NPI number obviously does nothing to improve patient care, how does promoting the adoption of the number fit the TDA’s mission? ***
8. - **During the 2008 Greater Southwest Dental Conference in Dallas, Delta Dental representatives routinely told dentists that the NPI number will be required for state licensure in Texas. Is that true?**

TDA staff has reviewed the TSBDE’s Application for Dental Licensure and the Application for Dental Licensure by Credentials available on the TSBDE website. Neither form requires a listing of an NPI number. (attachments 2 and 3)

9. - Does the TDA intend to contest misinformation that stakeholders tell Texas dentists regarding eDRs and HIPAA? *
10. - BCBSTX's NPI policy caused me to lose several families of long-term patients to dentists with NPI numbers. Have other TDA members reported losses as well? In your opinion, were my patients more likely helped or harmed by being forced from their dental home because of BCBSTX policy? *

To date, no TDA members, other than you, have reported patient loses due to the National Provider Identifier (NPI) requirement.

11. - Are there plans for the NPI number that have not been brought to the attention of TDA members?* For example, what does FOIA-disclosable information mean and how does it involve the NPI number, NPPES and pay-for-performance?

This question is addressed in part by the Centers for Medicare and Medicaid Services (CMS). The information below was taken from the CMS website. It is unclear how FOIA affects pay-for-performance.

Dissemination of Data from the National Plan and Provider Enumeration System (NPPES) Began September 4, 2007

NPPES health care provider data that are disclosable under the Freedom of Information Act (FOIA) will be disclosed to the public by the Centers for Medicare & Medicaid Services (CMS). In accordance with the e-FOIA Amendments, CMS has disclosed these data via the Internet. Data is available in two forms:

1. A query-only database, known as the NPI Registry.
2. A downloadable file.

CMS made FOIA-disclosable NPPES health care provider data available beginning Tuesday, September 4, 2007. The NPI Registry become operational on September 4th and CMS posted the downloadable file on September 12th.

Some of the key data elements that are FOIA-Disclosable are:

- NPI
- Entity Type Code (1-Individual or 2-Organization)
- Replacement NPI
- Provider Name (First Name, Middle Name, Last Name, Prefix, Suffix, Credential(s), OR the Legal Business Name for Organizations)
- Provider Other Name (First Name, Middle Name, Last Name, OR 'Doing Business As' Name, Former Legal Business Name, Other Name. for Organizations)
- Provider Business Mailing Address (First line address, Second line address, City, State, Postal Code, and Country Code if outside U.S., Telephone Number, Fax Number)

- Provider Business Location Address (First line address, Second line address, City, State, Postal Code, and Country Code if outside U.S., Telephone Number, Fax Number)
- Healthcare Provider Taxonomy Code(s)
- Other Provider Identifier(s)
- Other Provider Identifier Type Code
- Provider Enumeration Date
- Last Update Date
- NPI Deactivation Reason Code
- NPI Deactivation Date
- NPI Reactivation Date
- Provider Gender Code
- Provider License Number
- Provider License Number State Code
- Authorized Official Contact Information (First Name, Middle Name, Last Name, Title or Position, Telephone Number)

The delay in the dissemination of NPPES data does not alter the requirement that HIPAA covered entities must comply with the requirements of the NPI Final Rule no later than May 23, 2008. All NPI contingencies that may be in place must be lifted by that date.

Query-only Database (the NPI Registry)

UserIDs and passwords are not needed to use the NPI Registry. There is no charge to use the NPI Registry. It can be found at <https://nppes.cms.hhs.gov/NPPES/NPIRegistryHome.do>.

The NPI Registry operates in a real-time environment.

The NPI Registry enables users to query the NPPES by, for example, the NPI or the name of the provider. The NPI Registry will return the results of the query to the user, and the user will click on the record(s) he/she wants to see. The NPI Registry will then display the FOIA-disclosable data for those records.

Downloadable Files

There is no charge to download the files containing the NPPES FOIA-disclosable health care provider data. UserIDs and passwords are not needed to download these files.

The downloadable files contain the FOIA-disclosable NPPES health care provider data for health care providers who have been assigned NPIs. The current file is available at: http://nppesdata.cms.hhs.gov/cms_NPI_files.html. (An underscore precedes and follows "NPI".)

In October, CMS will make available a file that will replace the current file. This will be a full replacement file, not an update file. It will contain the FOIA-disclosable NPPES health care provider data as of a certain date which will reflect updates and changes that were applied to the NPPES records of enumerated health care providers between the date the first file was created and the date the full replacement file is created. When the

full replacement file is available for download, it will be the only file available for download. Update files will not be necessary. Because it will be a full replacement file, there will be no need to keep the first file available. CMS will follow this same procedure each month. As a result of this change, only one file will be available for downloading at any given time. This is an operational change from what is reflected in the NPPES Data Dissemination Notice and in our outreach documents, including the Frequently Asked Questions on NPPES data dissemination. This change will benefit users because it will eliminate any potential problems that users might have encountered in trying to develop ways to link updates, possibly from records that would have appeared in multiple monthly update files, to records that would have been included in the initial file.

Facts about the Downloadable File (the first file and all full replacement files):

1. The downloadable file is a Zip file that is a compressed archive file that contains (a) a "Read Me" document, (b) a Code Value document, (c) a Header File document, and (d) the FOIA-disclosable NPPES health care provider data file.
2. The data file (item (d) above) is a comma-separated value (CSV) file containing both the data and the header. Each data value is enclosed by a pair of double-quotes. If a data element does not have a value present, this will be indicated in the file by two double-quotes in a row.
3. The downloadable file is approximately 340 MB compressed (approximately 800 MB in size when decompressed).
4. It is intended that the file be downloaded and the data be imported into a relational database, or otherwise manipulated, by individuals with the requisite technical expertise.
5. Shareware text editors are recommended for users who wish to view the data file and/or perform simple searches. During testing, CMS was able to use Helios Textpad, Boxer Text Editor and Microsoft Access 2003 successfully to view the file.
6. There is no Help Desk or other technical support available from CMS, the NPI Enumerator, or any other CMS contractor for downloading, manipulating, or using the file.

Important Notes:

1. Contrary to our earlier NPPES data dissemination outreach information (including the FAQs), CMS has made the decision not to make FOIA-disclosable NPPES health care provider data available if the NPI has been deactivated. This means that the FOIA-disclosable data for a health care provider (individual or organization) who deactivated an NPI will not be found in the NPI Registry or in the downloadable file. CMS made this decision for three reasons: (1) deactivated records in NPPES cannot be viewed or edited by the health care providers who had been assigned those NPIs (these health care providers would have no way to update, change, or delete [where permitted] their FOIA-disclosable NPPES data); (2) covered entities should not use deactivated NPIs in standard transactions; and (3) health care providers who have deactivated their NPIs should not use, or allow others to use, their deactivated NPIs in standard transactions. If a health care provider cannot be located in the NPI Registry or the downloadable file, that health care provider either was not assigned an NPI or deactivated the NPI. FOIA-disclosable data for health care providers who

reactivate their NPIs will be displayed in the NPI Registry and will be included in the downloadable file. CMS will make a future determination as to the feasibility of creating a publicly available list of deactivated NPIs and the data that should be included in such files. If a determination is made to create such a list, CMS will make an appropriate announcement.

2. CMS must temporarily suppress the Employer Identification Numbers (EINs) of organization providers. CMS has discovered that some providers reported SSNs in the EIN field. We expect that this reporting was done primarily by incorporated individuals and sole proprietors who applied for NPIs as organizations. CMS does not want to risk the disclosure of any provider's SSN. CMS will undertake efforts to have this problem resolved. Once CMS believes that to be the case, we will display organizations' EINs in the downloadable file and in the NPI Registry.
3. The NPPES Data Dissemination Notice and outreach documents from CMS encouraged health care providers to review their FOIA-disclosable NPPES data and edit it as necessary and to remove, if they wished, sensitive data from FOIA-disclosable fields that were furnished on an optional basis (i.e., data that were not required to be furnished in order to apply for an NPI). Many health care providers have taken some or all of these actions. To further help ensure non-disclosure of Social Security Numbers (SSNs) and IRS Individual Taxpayer Identification Numbers (ITINs), CMS is suppressing from display in the NPI Registry and in the downloadable files any SSNs or IRS ITINs that remain in any of the FOIA-disclosable fields in the records of health care providers who are individuals.

Special Note for Health Care Providers:

The NPI Registry and the downloadable files will contain data from the NPPES as reported to NPPES by you, or by someone acting on your behalf, or by an organization provider's Authorized Official. Please read Important Notes 2 and 3, above. If the downloadable file or the NPI Registry reflects information that is incorrect, health care providers should correct that information. At any time, providers, or someone acting on their behalf, may edit their records by going to <https://nppes.cms.hhs.gov>, or by obtaining a paper NPI Application/Update Form (CMS-10114) from the NPI Enumerator or from the CMS forms page (www.cms.hhs.gov/cmsforms), completing it, and mailing it to the NPI Enumerator. Providers who need assistance in editing their records should contact the NPI Enumerator by phone at 1-800-465-3203, by email customerservice@npienumerator.com, or by letter: NPI Enumerator, P.O. Box 6059, Fargo, ND 58108-6059.

Informational Documents on the Data Dissemination File

Three new documents are available in the Downloads section below; these documents relate to the file containing NPPES health care provider data (see NPPES Data Dissemination Notice, published May 30, 2007, also available in the Downloads section below). This file will be available for download from an Internet site in early September 2007. These three documents will also be part of that downloadable file. We are making them available separately, in advance, in response to requests from the industry. They are:

- Data Dissemination File - Code Values,
- Data Dissemination File - Read Me
- NPIData 20050523-20070710FileHeader

FOIA-Disclosable Data Elements

The document entitled, "National Plan and Provider Enumeration System (NPPES) Data Elements – Data Dissemination – Information for Providers," dated June 20, 2007, will assist providers in knowing which of the FOIA-disclosable data can be updated, changed, or deleted. This document is located in the Downloads Section below.

Reference: Centers for Medicare & Medicaid Services. Website. CMS
 Home>Regulations and Guidance>National Provider Identifier Standard>Data
 Dissemination Available from: URL:
http://www.cms.gov/NationalProviderStand/06a_DataDissemination.asp

12. - If a dentist volunteers for an NPI number and later changes his or her mind, is it possible to back out of the mandate without fear of retaliation from HHS?

Dentists as well as other health care providers are permitted to deactivate their NPI numbers. CMS did not address retaliation in its answers to questions listed in the NPI FAQ section of the website. Please see questions and answers below.

When should a health care provider deactivate its NPI?

Published 04/27/2007 12:34 PM | Updated 05/24/2010 07:09 AM | Answer ID 8382

When should a health care provider **deactivate** its NPI?

A health care provider (or the trustee/legal representative of a health care provider) should **deactivate** its NPI in certain situations, such as retirement or death of an individual, disbandment of an organization, or fraudulent use of the NPI. To **deactivate** an NPI, a health care provider (or the trustee/legal representative of a health care provider) must complete a CMS-10114 and mail it to the NPI Enumerator.

Reference: Centers for Medicare & Medicaid Services. Website. CMS
 Home>Regulations and Guidance>National Provider Identifier Standard>NPI
 Frequently Asked Questions (FAQs) from: URL:
http://questions.cms.hhs.gov/app/answers/detail/a_id/8382/kw/deactivation

If a health care provider deactivates its National Provider Identifier (NPI), will its record still be in the downloadable file and the query-only database? How will it be known that the NPI was deactivated?

Published 05/24/2007 11:49 AM | Updated 03/04/2010 02:16 PM | Answer ID 8444

If a health care provider **deactivates** its National Provider Identifier (NPI), will its record still be in the downloadable file and the query-only database? How will it be known that the NPI was **deactivated**?

No. Neither the downloadable file nor the query-only database will contain information about health care providers whose NPIs are **deactivated**. **Deactivated** NPIs should not be used in standard transactions. CMS may determine at a later date to make available a list of **deactivated** NPIs. If that determination is made, CMS will provide appropriate information in an announcement that will be posted on the CMS NPI web page.

Reference: Centers for Medicare & Medicaid Services. Website. CMS Home>Regulations and Guidance>National Provider Identifier Standard>NPI Frequently Asked Questions (FAQs) from: URL: http://questions.cms.hhs.gov/app/answers/detail/a_id/8444/kw/deactivation

13. - How much does it cost for a solo practitioner to be 100% HIPAA compliant?

The cost for a solo practitioner to be 100% compliant will depend on variations in practice size and type of compliance assistance needed.

14. - What percentage of Texas dentists are HIPAA compliant?

HIPAA enforcement is primarily a complaint-driven process. Both the Office for Civil Rights (OCR) and the Centers for Medicare and Medicaid Services (CMS) offer technical assistance to help covered health care providers voluntarily comply with HIPAA. Since covered providers are not required to "register" with either OCR or CMS, there is no repository of information as to what percentage of Texas dentists are HIPAA compliant.

15. - Is HIPAA effective?*

16. - Does the HIPAA Privacy document that dentists require new patients to sign perform provide tangible benefit? When patients sign mandated forms such as this, is it cost-effective even if they don't take the time to read them?

According to the Office for Civil Rights, the HIPAA Privacy Rule requires a covered health care provider to give every patient of record their Notice of Privacy Practices no later than the first date of treatment and to make a good faith effort to obtain the patient's written acknowledgment of receipt of the notice. Although we recognize that cost may be an issue for dental offices; the Privacy Notice is part of the overall Privacy Rule, and covered health care providers must comply.

Data Breaches

17. - In 2009, how many dental practices in Texas suffered data breaches? Is the number increasing or decreasing?

The TDA does not collect this information.

18. - How many computers containing PHI were stolen in burglaries of Texas dental offices in 2009?

The TDA does not collect this information.

19. - How many breaches, whether by burglary, hacker or dishonest employee involved more than 500 patients?

As you reported in your article on the website www.medicalexecutivepost.com; the following breaches involving more than 500 patients have been reported to the Secretary of the US Department of Health and Human Services [DHHS].

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>

<http://medicalexecutivepost.com/2010/02/24/protected-health-information-data-breaches/>

20. - How much money have breaches cost dentists in Texas?

That number may be impossible to quantify as you yourself have addressed in several online postings listed below.

-Posted on November 28, 2008-***The Ponemon Institute Report*** A couple of years ago, the Ponemon Institute estimated that it costs almost \$200 per patient to do this. For a small dental practice with only 2500 active patients, that is half a million dollars – even before the fines arrive. **Economic Costs** But wait, there is more. If the immediate financial costs do not bankrupt the practice, Ponemon once estimated that 20% of the clients will never return to a business that fumbled their identity. I think Ponemon is an optimist. Ponemon's estimate is not based on breaches from dental practices. I think at least a third of dental patients would immediately leave and probably seek out a dentist who uses paper records. And that is when they will find me." From:

<http://medicalexecutivepost.com/2008/11/28/much-more-on-dentistry-and-the-ehr-controversy/>

- Posted on September 27, 2009 at 8:52pm "Let's get the obscene stuff over with first. I read today that the Ponemon Institute estimates that a breach will cost a provider \$202 per patient. Their research is quoted in the Interim Final Rule for Notification. (See "Long term costs for a breach of just 499 records could be as high as \$100,798" - ExperiorData Healthcare Security & Encryption press release)

<http://www.experiordata.com/blog/?p=94>

The direct costs of notifying patients and covering their credit reports for a few years is only \$50 per patient. However, the long term reputational damage costs \$152 per patient. If the breach involves more than 500 patients, the costs per patient go up because then local news media have to be informed of the unfortunate accident. A breach could cost the average dentist a million dollars or more, even before the lawsuits. (Gasp!)" From: <http://community.pennwelledentalgroup.com/forum/topics/hipaa-fines-and-other>

-Posted on November 15, 2009 –**“Two Hundred Ten Dollars Cost – Per Record – for Notification** Considering that in October, the Ponemon Institute reported that it costs an estimated \$210 per record to notify patients of a breach, there are a lot of angry lawmakers who are missing the point. Mandated fines for a breach are meaningless. Simply notifying thousands of patients of a breach will bankrupt any dental practice, even if it is an insurance company employee who loses a laptop computer containing a dentists’ patients’ personal data – like a BCBS employee did recently with over 800,000 physicians’ personal information.” From: <http://medicalexecutivepost.com/2009/11/15/don%E2%80%99t-hide-a-security-breach-if-you-can%E2%80%99t-do-the-time/>

-Posted on February 23, 2010 at 2:36pm- **“Do you know what the burglary will cost Ashley and Gray? According to the Ponemon Institute, just to notify their 9000 patients at \$50 a person will cost almost half a million dollars. But that’s hardly the end of the hurt. Consider the harm the burglar did to the dentists’ reputations. The Ponemon Institute estimates that the fumbled PHI will cost the dentists \$150 x 9000 = \$1.35 million in lost production. The Missouri dentists were bankrupt even before HHS inspectors arrived at their office - working on commission. I’m certain they have completed their investigation of proper documentation of HIPAA busywork. The dentists’ level of documentation will be important evidence in determining if the burglary was caused by willful neglect.”** From: <http://community.pennwelldentalgroup.com/forum/topics/hhs-reports-a-missouri-dental>

21. - Have there been any dentist bankruptcies attributed to data breaches?

The TDA does not collect this information.

22. - Does Texas Attorney General Greg Abbott intend to sue HIPAA-covered entities who experience data breaches? (Attorneys General in other states are doing this).

The Texas Attorney General's office has posted an extensive listing of major lawsuits and settlements on its website. Of those listed, some address identity theft issues, specifically the cases involving CVS, EZ Pawn, and RadioShack. For a complete listing, and to read more about the cases mentioned above please visit: <http://www.oag.state.tx.us/consumer/lawsuits.php#68>

TDA complaint resolution

Re: questions 23-28. Information of this nature regarding members is not made available by the TDA. We know of no lawsuits by members.

23. - What percent of TDA members’ complaints against TDA officers and employees are satisfactorily resolved?

24. - What percent of unresolved complaints results in TDA members quitting the organization?

25. - What percent result in lawsuits?

26. - What percent of TDA officers' and employees' complaints against members are satisfactorily resolved?

27. - What percent of unresolved complaints results in TDA members quitting the organization?

28. - What percent result in lawsuits?

29. - What percent of TDA employees' complaints against officers are satisfactorily resolved?

There have been none.

30. - What percent of TDA employees subsequently quit or otherwise terminated?

Not applicable.

31. - What percent result in lawsuits?

Not applicable.

Representation

In the January 2010 TDA Journal, Dr Patricia L. Blanton, Vice Chairman, XV Trustee District and Chairman of the Planning and Review Committee, published "Power in the 'Present'" in which she was quite frank in her criticism of poor representation of members' interests on a national level, and promised changes. She reports, "As a result of a recent planning effort, the XV District delegation has identified four strategic goals."

1. Educate - Provide a forum for the delegates to be informed and promote discussion of the issues.

2. Resolve - Develop issues and resolutions to influence the policies and influence of the ADA.

3. Consensus Build - Develop strategy to ensure that the mission of the XV is successful.

4. Represent - Properly represent the interests of the patients and dentists of Texas.

32. - What is the progress on the delegation's goals four months later? I would suggest that a simple, transparent TDA Facebook page will accomplish all four of your goals naturally.

Dr. Jerry Long, the Fifteenth District Trustee, has appointed four committees for each of the areas listed above. To date, the committees have not issued reports.

33. - In October, ADA Delegates will vote on House Resolution 82 that was presented to the House this fall. It is an unprecedented and incredibly vague ADA Members Code of Conduct along with unexplained sanctions that will be brought against guilty

members by ADA leaders. If there are delegates from Texas who support the adoption of the code and sanctions, what are their names?

The Texas Delegation does not vote in a block. Voting is done individually and TDA does not pre-poll its delegates as to how they will be voting.

- 34. - For years, I asked TDA officials numerous questions on the TDA Forum, and only one officer replied. Why do leaders not respond to questions on even a private forum?**

Participation on the TDA Forum is voluntary. Members and/or leaders are not mandated to post or answer questions on the forum.

- 35. - Finally, after all we've been through, why am I still not allowed on the TDA Facebook? Some may find me objectionable, but my dental patients need me to help you with your social networks, otherwise their interests will never see the light of day. As far as I can tell, I'm the most effective advocate you have.**

The TDA Facebook page was created as a means to communicate association information in a timely, succinct manner with our members. It is, and was never intended to be a vehicle by which one member dominates content. You have expressed on many occasions that your intent was to dominate, control content and/or eventually shut the page down. Additionally, you created a false Facebook page identity under the name, "John Hamm" which is a violation of Facebook rules and also conducted a game on the TDA Facebook page without TDA's permission. As we have previously told you, in order to continue the TDA Facebook group, we must abide by the Facebook Terms of Use and Statement of Rights and Responsibilities.

New Patient Privacy Regulations Take Effect Soon: How do HIPAA and State Privacy Laws Affect Your Practice?

During the next 12 months, a series of federal regulations and a new state law will impose new requirements on all Texas dentists. These laws and regulations are intended to protect patient privacy and the confidentiality of health information. Texas dentists should learn more about them — after all, we're all patients as well as providers.

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, is a federal law designed to protect the confidentiality and security of patient information, encourage electronic commerce in the health care industry, and ultimately simplify the process by which that commerce is transacted. HIPAA regulations do not require dentists and other providers to submit transactions electronically, but they do require that transactions submitted electronically comply with certain standards. As part of that effort, HIPAA establishes standards for electronic transmission of health care transactions, privacy standards to protect the confidentiality of a patient's personal health care information, and security standards to protect against deliberate or inadvertent misuse or disclosure of individually identifiable health information.

Does my practice need to comply?

According to the ADA, many dentists are considered a "Covered Entity" under HIPAA — a healthcare provider who transmits certain health information (including claims) in electronic form, either directly or indirectly, through a vendor or billing service. Under HIPAA, the term "Electronic Health Transactions" includes the electronic transmission of health claims, health plan eligibility, enrollment and disenrollment, payments for care and health plan premiums, claim status, first injury reports, coordination of benefits, and related transactions.

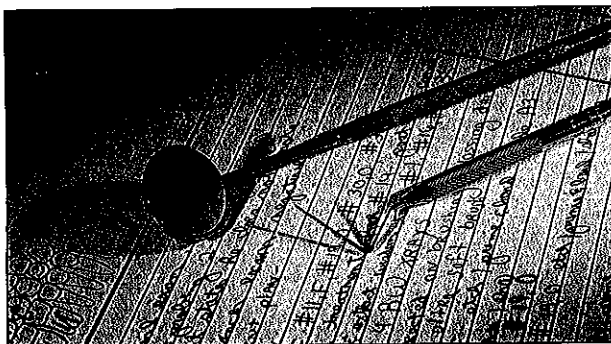
Although HIPAA itself may not apply to you, a new Texas law, the Texas Medical Privacy Act (TMPA), will take effect next year and impose HIPAA-like requirements on every dental office in Texas. (See below for more about TMPA.)

HIPAA compliance deadlines are right around the corner. Is your dental practice prepared?

Electronic Transactions Standards — October 16, 2002.

The deadline for compliance with the Electronic Transactions standards is October 16, 2002. However, delays in finalizing the rules have made it nearly impossible to comply with the original deadline. As a result, the ADA recommends that dentists submit an application for an extension — a "compliance plan" — by October 15, 2002. Filing the compliance plan extends the deadline until October 16, 2003. The easiest way to file for an extension is to use the online compliance plan from the Center for Medicaid and Medicare Services' (CMS) Web site at <http://www.cms.gov/hipaa/hipaa2/ASCAForm.asp>. CMS provides an online confirmation number to acknowledge receipt of electronic extension applications. Dentists should keep this verification of submission. CMS will not acknowledge receipt of paper submissions. If you mail your extension application, request a return receipt from the U.S. Postal Service.

Please note that this extension applies to the Electronic Transactions standards only. It does not affect any other HIPAA compliance deadlines.



Privacy Standards — April 14, 2003.

Dentists and other health care providers covered by HIPAA are required to comply with the privacy standards by April 14, 2003. The American Dental Association (ADA) advises that you start right way to develop written privacy forms and notices for your office. They suggest conducting a "gap analysis" to help you understand the requirements of the law and your current practice activities. Once you have your forms and notices, the ADA also advises dentists to start obtaining a signed "Acknowledgement of Receipt of Notice of Privacy Practices" from each of your patients. In addition, you should train your dental team about your privacy policies and procedures, and designate two individuals in your office to serve as a privacy officer and a contact person to receive complaints.



Security Standards — Deadline to be determined.

HIPAA includes a third set of standards governing security, to protect against the deliberate or inadvertent misuse or disclosure of individually identifiable health information. According to the ADA, federal officials have yet to develop the security standards. Once developed, the standards will take effect 2 years and 60 days after publication.

What about new Texas laws?

Texas Medical Privacy Act — September 1, 2003.

In 2001, the Texas Legislature enacted a new law protecting the confidentiality of patients' medical information, the Texas Medical Privacy Act (TMPA), which is codified as Chapter 181 of the Texas Health and Safety Code. According to TDA's legal counsel, if a health care provider complies with HIPAA, that provider should be in compliance with TMPA.

TMPA covers more entities than HIPAA, however, and is likely to affect nearly all Texas dentists. Under TMPA, "Covered Entities" generally includes any person or entity that "uses, collects, stores, transmits, assembles, analyzes, evaluates, comes into possession of, obtains, or stores" protected health information for essentially any reason. The definition of covered entities under TMPA also includes many entities that would have been considered "business associates" under HIPAA.

Since TMPA was enacted, other than provisions of the statute itself, TDA has been able to obtain little legal or industry guidance to interpret or ascertain its applicability. Despite this lack of guidance, compliance with TMPA is required by September 1, 2003. Working with our legal counsel, TDA will continue to monitor implementation of the new law and keep members informed about its implications for dentistry in Texas.

ADA and TDA are here to help.

The TDA leadership and staff work hard to stay abreast of developments related to both HIPAA and TMPA and continue to provide information and guidance in *TDA Today*, the *Texas Dental Journal*, and on the TDA Web site, www.tda.org.

The TDA Web site features links to a variety of HIPAA-related information. The ADA also offers a "HIPAA Privacy Kit" that includes a compliance checklist, sample privacy forms, and a set of easy-to-understand policies and procedures. The kit costs \$125 and is available from the ADA by calling (800) 947-4746.

In addition, TDA's Council on Dental Education, Trade & Ancillaries will host an "ADA HIPAA Compliance Meeting" on December 13, 2002 at the LBJ Auditorium on the University of Texas campus in Austin. Registration information is available now on the TDA Web site accessed via the member homepage on the professional side of the site. For more information, contact Diane Rhodes at drhodes@tda.org or (512) 443-3675. ★



Texas State Board of Dental Examiners
 333 Guadalupe, Tower 3, Suite 800
 Austin, Texas 78701-3942
 Phone: (512) 463-6400 / Fax: (512) 463-7452
 Website: www.tsbde.state.tx.us
 E-Mail: information@tsbde.state.tx.us

Application for Dental Licensure

Instructions:

- Print or type all information. All incomplete applications will be returned without action.
- Fees are Non-Refundable. The SBDE accepts Personal Checks, Cashiers Check or Money Orders. Do not send cash. Make your payment to the Texas State Board of Dental Examiners (SBDE).
- The following **must** be completed **before** you mail this application to the SBDE: (Instructions for these steps are found on Page 3 of this application)
 1. Complete the required Fingerprint Criminal Records Check.
 2. Complete the required SBDE Jurisprudence Assessment for Initial Licensure.

FEES

- LICENSURE BY EXAMINATION: **\$400**
OR
LICENSURE FOR GRADUATES
- OF NON-ACCREDITED **\$400**
DENTAL PROGRAMS:
OR
- TEMPORARY LICENSURE: **\$700**

I AM APPLYING FOR: _____ LICENSURE BY EXAM OR _____ TEMPORARY LICENSURE OR _____ LICENSURE FOR GRADUATES OF
 _____ NON-ACCREDITED DENTAL PGMS.

PERSONAL INFORMATION

- DATE: _____
- SOCIAL SECURITY NUMBER: _____
- FIRST NAME: _____
- MIDDLE NAME: _____
- LAST NAME: _____
- LIST ALL FORMER NAMES: _____
- DATE OF BIRTH: _____
MM/DD/YY
- HOME ADDRESS: _____
- CITY: _____ STATE: _____ ZIP: _____ COUNTRY: _____
- MAILING ADDRESS: _____
- CITY: _____ STATE: _____ ZIP: _____ COUNTRY: _____
- DAYTIME PHONE: _____
- ALTERNATE PHONE: _____

PRACTICE INFORMATION

- PRACTICE: GENERAL DENTIST _____
- TYPE OF PRACTICE: PRIVATE _____ MILITARY _____
SPECIALTY _____ FACULTY _____ PUBLIC HEALTH _____

DENTAL EDUCATION

- SCHOOL ATTENDED: _____
- DENTAL DEGREE: _____
- YEAR GRADUATED: _____

POST GRADUATE TRAINING

- SCHOOL ATTENDED: _____
- TYPE OF PROGRAM: _____
- YEAR GRADUATED: _____

PRINT YOUR NAME ON THE LINE BELOW AS YOU WISH IT TO APPEAR ON YOUR LICENSE

(PLEASE PRINT LEGIBLY)

(Continued on the Next Page)

STATE LICENSURE/JURISDICTIONS

(List all states/jurisdictions in which you are or have been licensed)

State: _____	License Number: _____	License Issue Date : _____	Disciplinary Action? _____
			Yes _____ No _____
State: _____	License Number: _____	License Issue Date : _____	Disciplinary Action? _____
			Yes _____ No _____

TEXAS NON-PROFIT CORPORATION EMPLOYER

(For Temporary Licensure Applicants Only)

Corporation Name: _____	Supervisor Name: _____
Address: _____	Supervisor Phone Number: (_____) _____
_____ City _____ State _____ Zip Code _____	Employer Medicaid Provider Identification Number: _____

BACKGROUND INFORMATION

A "yes" answer to any question listed below requires additional information. Please submit a dated and signed letter of explanation and any appropriate legal disposition papers.

____ Yes ____ No Have you ever held a license issued by the State Board of Dental Examiners (SBDE)?
If yes, include the type of license and license number:
License Type: _____ License Number: _____

____ Yes ____ No For any criminal offense, including those pending appeal have you:

- A. Been convicted of a misdemeanor;
- B. Been convicted of a felony;
- C. Received deferred adjudication;
- D. Been placed on court-ordered probation;
- E. Been sentenced to serve jail or prison time or court-ordered confinement;
- F. Been arrested or have any pending criminal charges;
- G. Been subject to a court martial; Article 15 violation; or received any form of military judgment/punishment/action.

(You may exclude only Class C misdemeanor traffic violations)

Note on Expunged and Sealed Offenses: While expunged or sealed offenses, arrests, tickets, or citations need not be disclosed, it is your responsibility to ensure the offense, arrest, ticket, or citation has, in fact, been expunged or sealed. It is recommended that you submit a copy of the Court Order expunging or sealing the record in question to our office with your application. Failure to reveal an offense, arrest, ticket, or citation that is not in fact expunged or sealed, could at a minimum, subject your license to a disciplinary fine. Non-disclosure of relevant offenses raises questions related to truthfulness and character.

____ Yes ____ No Are you currently the target or subject of a grand jury or governmental investigation?

____ Yes ____ No Has any licensing authority refused to issue you a license or ever revoked, annulled, cancelled, accepted surrender of, suspended, placed on probation, refused to renew a license, registration, or certificate held by you now or previously, or ever fined, censured, reprimanded or otherwise disciplined you?

____ Yes ____ No Within the past five (5) years have you been addicted to and/or treated for the use of alcohol or any other drug?

(Continued on the Next Page)

REQUIRED DOCUMENTATION (Applications that do not include documentation listed below will be returned without action)

All Applicants must submit the following documentation (#1 through #9):

1. Xerox copy of receipt issued by L1 Enrollment Services showing proof of having your fingerprints collected for the required fingerprint criminal records check. Information on this process is available at: www.tsbde.state.tx.us/Fingerprint
2. Xerox copy of official birth certificate, passport, or naturalization papers. Copies of hospital birth records are not acceptable.
3. Proof of graduation from dental school, i.e., certified or notarized copy of diploma or a certification from school.
4. Proof of passing National Board examination, i.e., certified or notarized copy of certificate or computer score card.
5. Proof of passing clinical examination i.e., certified or notarized copy of examination results. WREB results must be dated within the last five years. CRDTS results must be dated after within the last five years; NERB or SRTA results must be dated after January 1, 2005.
6. Verification letter with imprint of state seal from the dental board in each state in which licensure is/was held. (A copy of the license alone is not acceptable). This is only applicable to applicants who hold other state licenses.
7. Xerox copy of current (as indicated on card) basic life support CPR certification card. CPR training must include a written assessment and a demonstration of skills. Computer and video-based CPR training courses given by an instructor that include a hands-on practice manikin and a written assessment of skills, either taken online or in a classroom setting, are acceptable. Online courses that do not include a live instructor for a demonstration of skills are not acceptable.
8. Proof of successful completion of SBDE Jurisprudence Assessment for Initial Licensure. Information on taking the SBDE Jurisprudence Assessment can be found at: www.tsbde.state.tx.us/Jurisprudence. Your Jurisprudence Assessment Certificate of Completion must be dated within preceding twelve (12) months. (A Xerox copy of the Certificate of Completion is is acceptable)
9. Proof of Social Security Number (Copy of card is acceptable) To obtain a Social Security Number visit: www.socialsecurity.gov/ssnumber/

Foreign Graduate Applicants: In addition to submitting documents #1 through #9, also submit the documentation listed at Letter A below:

- A. Proof of completion of ADA approved specialty training program. A certified or notarized copy of program completion certificate or original certification letter from the Program Director is acceptable.

Temporary Licensure Applicants: In addition to submitting documents #1 thru #9, also submit the documents listed at Letters AA through DD below:

- AA. Verification of dental employment with a Texas Non-Profit Corporation that accepts Medicaid reimbursement. (Attach copies of articles (including any amendments) of incorporation as a non-profit corporation.)
- BB. Verification from employer that a Medicaid Identification Number has been issued and is current.
- CC. Proof of 12 hours technical or scientific continuing education, in accordance with SBDE Chapter 104, dated within the last 12 months.
- DD. Report from the National Practitioner Data Bank or American Association of Dental Examiners (must be dated within 6 months of application date)

In addition to the foregoing:

I acknowledge this is a legal document and I attest that I understand and meet all the requirements to practice for the type of licensure requested. Further, I understand that it is a violation of the Texas Administrative Code and the Penal Code to submit a false statement to a government agency and:

I consent to the release of confidential information to the Texas State Board of Dental Examiners and further authorize the Board to use and to release said information as needed for the evaluation and disposition of my application for licensure.

Applicant's Signature

STATE OF _____

COUNTY OF _____

Before me, the undersigned authority, on this day personally appeared the applicant whose signature appears above and who being by me sworn upon oath says that all the facts, statements and answers contained in this application are true and correct.

Sworn and subscribed to before me, the said _____
appeared on this the _____ day of _____, 20 _____, to certify which witness my hand and seal of office.

Notary Public

(seal)



Application for Dental Licensure by Credentials

Texas State Board of Dental Examiners
333 Guadalupe, Tower 3, Suite 800
Austin, Texas 78701-3942
Phone: (512) 463-6400 / Fax: (512) 463-7452
Website: www.tsbde.state.tx.us
E-Mail: information@tsbde.state.tx.us

Fee: **\$2,500**
(PERSONAL CHECK, CASHIERS CHECK
OR MONEY ORDER – NO CASH PLEASE)

PERSONAL INFORMATION

First Name: _____ Middle Name: _____ Last Name: _____
Mailing Address: _____ Social Security #: _____
City: _____ State: _____ Zip: _____
Daytime Phone: _____ Alternate Phone: _____

REQUIRED DOCUMENTATION

Attach the following documents and appropriate fee to this application and submit to the Texas State Board of Dental Examiners office at the address above. Applications not having these documents will be returned to the applicant.

- Letter from PBIS to you confirming your package has been forwarded to the State Board of Dental Examiners.
- Proof of Social Security Card. Xerox copy of card is acceptable.
- Proof of successful completion of SBDE Jurisprudence Assessment dated within the preceding 12 months. The Jurisprudence Assessment can be purchased and taken online at: www.tsbde.state.tx.us/Jurisprudence
- Twelve hours of continuing education taken within the preceding 12 months in accordance with Chapter 104 of the SBDE Rules and Regulations.

I hereby declare under penalty of perjury the information included in this application to be true and complete to the best of my knowledge. In signing this application, I am aware that a false statement or evasive answer to any questions may lead to denial of my application or subsequent revocation of licensure on ethical grounds. I accept the laws and rules of the Dental Practice Act and State Board of Dental Examiners Rules and Regulations as the basis for lawful dental practice in the State of Texas.

Applicant's Signature

Date

STATE OF _____

COUNTY OF _____

Before me, the undersigned authority, on this day personally appeared the applicant whose signature appears above and who being by me sworn upon oath says that all the facts, statements and answers contained in this application are true and correct. Sworn and subscribed to before me, the said _____ appeared on this the _____ day of _____, 20 _____, to certify which witness my hand and seal of office.

NOTARY PUBLIC
(seal)