EXECUTIVE-POST
[www.HealthcareFinancials.wordpress.com]

HIPAA Rules and Dentistry

A Survey of Dentists [Pilot Study]
By Darrell Pruitt; DDS

A survey of 18 dentists was performed using the Internet as a platform. The volunteer dentists' anonymity was guaranteed. The dentists were presented with ten HIPAA compliancy requirements followed by a series of questions concerning their compliancy as well as the importance of the requirements in dental practices.

The range of compliancy was found to be from 0% for the requirement of a written workstation policy to 88% for that of password security. The average was 49%, meaning that less than half of the requirements are being respected by the dentists in this sample.

Frustration with the tenets of the mandate, as well as open defiance is evident by the written responses. In addition, it appears that a dentist's likelihood of satisfying a requirement is related to the dentist's perceived importance of the requirement.

Even though this is a limited pilot study, there is convincing evidence that more thorough investigation concerning the cost and benefits of the requirements need to be performed before enforcement of the HIPAA mandate is considered for the nation's dental practices.

Introduction

Beginning more than a decade ago, dentists in the nation were told to prepare for HIPAA inspections. We were warned of the tremendous fines that can be assessed by the US Department of Health and Human Services if a dental practice is found to be in violation of the law. The attention forced many dentists to consider their responsibility to protect their patients' identities - causing some to install passwords for the first time and to pay closer attention to who was using their office computers.

However, mixed with the good advice, there were also rumors based on interpretations of the arguably vague law. Some dentists were told that "open bay" office designs would be forever outlawed because they unavoidably infringe on patients' privacy. It was also suggested that allergy stickers, if visible on the outside of charts, should be color-coded to prevent passers-by from accidentally obtaining someone else's private medical information.

Since it is difficult for dentists to find reliable information about HIPAA, the question must be asked: Are dentists in the nation maintaining HIPAA compliancy? More importantly, are the recommended procedures effective at fulfilling their intended purposes?

On the following pages are ten HIPAA requirements followed by questions which were answered by 18 dentists in a survey conducted on a web application provided by Tacilent, a knowledge management company located in Dallas. **http://www.tacilent.com/**

The first nine requirements were copied from an article titled "Demystifying HIPAA: Part III—Physical Safeguards of the Security Rule," written by HIPAA consultant Olivia Wann; RDA, BSHCA. It appeared in the November 2007 issue of *Contemporary Oral Hygiene*. **http://www.contemporaryoralhygieneonline.com/issues/articles/2007-11_03.asp**

The tenth requirement concerns the Notice of Privacy Policy (NPP) form, and is from the US Department of Health and Human Services. **http://www.hhs.gov/news/facts/privacy.html**

Methods

Twenty dentists, all acquaintances of the lead researcher, were contacted by phone and asked to take part in a survey concerning the relevance of HIPAA in their dental practices. A few days later, they were provided them with a username and password which allowed them to log on to Tacilent's web application for research. Since the participants' identities are unknown, their anonymity is guaranteed – allowing them to respond without fear of embarrassment or incrimination.

Results:

1. Contingency plan for office access and equipment

"Only authorized team members should have access to the dental office and its equipment. Someone on staff should be assigned to make certain that the doors and windows are locked each day. File server cabinets should be locked. As a consultant, I recommend not housing the file server on a basement level or in an area susceptible to flood (i.e., near pipes that could break or a sink that could overflow)." Ms. Wann adds; "Alarm systems are extremely desirable to detect intrusion, especially for those dental offices located in high crime areas. Some systems use computer software that allows the practice owner to view the office through the Internet."

Question 1: A Contingency plan must be made in advance to avoid a compromising situation in the event of an emergency. Does your practice have a security plan?
Yes: 41% (7of 17)
No: 53% (9)
No answer: 6% (1)

Question 2: If no, are you preparing to implement a plan?
Yes: 22% (2 of 9)
No: 78% (7)

Question 3: If you are not implementing a security policy at this time, why not?

- "I am not a HIPAA covered entity. However I do respect both security and privacy."
- "We don't know how."
- "All records are kept in written form with access only by the staff."
- "No windows, one door, no pipes near computer or backup discs, only one office person uses computer."

2. Facility security

"The office's policies should detail who has access to the facility. It is appropriate to ask for proof of identity before allowing access to the dental office. For example, if the office consults with a new computer hardware company, the security officer may require the technical specialist to present identification to verify the person's identity."

Question 1: Does your practice have a facility security policy?
Yes: 56% (10 of 18)
No: 44% (8)

Question 2: If no, are you preparing to implement a policy?
Yes: 13% (1 of 8)
No: 88% (7)

Question 3: If you are not implementing a facility security policy at this time, why not?

- "Don't know how."
- "All records are written and can only be accessed by someone behind the front desk."
- "In reality I don't see the importance of the formality. People don't care if someone is allergic to something."
- "I am not using an outside consultant to view my computer data."
- "Feel it is not needed."

3. Maintenance documentation

"Documentation of maintenance is necessary and must include the date, type of repair, and who authorized it. If the technician repairs the computer or device off site, notation should be made in the dental office's records."

Question 1: Do you practice document maintenance performed on your computers?
Yes: 18% (3 of 17)
No: 77% (13)
No answer: 6% (1)

Question 2: If no, do you intend to adopt a document maintenance plan in the future?
Yes: 46% (6 of 13)
No: 54% (7)

Question 3: Rank the importance of documenting maintenance (3 being the highest).
Average rank 1.5 (midway between zero and 3)

Question 4: If you are not documenting maintenance at this time, why not?

- "We have a maintenance contract with a company that maintains upgrades, etc. and they have the records which are available to us."
- "We know and trust the IT / repair person."
- "We don't send our computers out to be repaired."
- "All maintenance is done on-site."
- "I have not had to have any maintenance on our computers since we instituted HIPAA policies."
- "Have not been forced to yet"
- "Documentation is automatic with billing statements."
- "Probably should be added (a log), but the repair guy has signed a HIPAA agreement."

- "Excessive paper work; my billing from my hardware & software vendors is sufficient for my needs."

4. Use of computer workstations

"The dental office's policy should detail the appropriate use of computer workstations, regardless of where they are located. Operatory workstations should not be logged on and left unattended. For example, if the assistant leaves the treatment room, precautions should be taken to prevent the patient from accessing the computer and viewing other patients' information. Additionally, each computer should be set up to automatically log off after a certain number of minutes of inactivity."

Question 1: Does your practice have a written workstation policy?
Yes: 0% (0 of 17)
No: 100%

Question 2: If no, do you intend to create one?
Yes: 29% (5 of 17)
No: 71% (12)

Question 3: How would you rank the importance of a workstation policy?
Average rank 1.1

5. Password security

"If a dentist uses a notebook computer or personal digital assistant, a password should be added to prevent unauthorized access if the device is stolen. I recently consulted in a hospital where a physician habitually left his computer workstation logged on to the network. In the evenings, the janitor was accessing the system. This violation was reported to the HIPAA security team and immediate corrections were made."

Question 1: Does your practice use passwords?
Yes: 88% (15 of 17)
No: 12% (2)

Question 2: If no, do you intend to assign passwords?
Yes: 0% (0 of 2)
No: 100% (2 of 2)

Question 3: How would you rank the importance of passwords to security?
Average rank: 2.0

Question 4: Do you think a password is an effective safeguard if a computer is stolen?
Yes: 41% (7 of 17)
No: 59% (10)

Question 5: Do you think encryption is an effective safeguard if a computer is stolen?
Yes: 71% (12 of 17)
No: 29% (5)

6. Firewall and antivirus

"It is highly important that the antivirus software be updated routinely to avoid expiration. Additionally, firewalls should be in place to help prevent someone from hacking into the system."

Question 1: Is your antivirus software and firewall functional and updated routinely?
Yes: 71% (12 of 17)
No: 24% (4)
No answer: 6% (1)

Question 2: If not, do you intend to upgrade?
Yes: 0% (0 of 4)
No: 75% (3)
No answer: 25% (1)

Question 3: Do you feel that you have acceptable software/firewall security measures in place? How important is this?

53% (9 of 17) stated that software/firewall security is very important.
24% (4 of 17) commented that their computers were not connected to the Internet.

- "Extremely important ... hackers know more than the mere dentist and staff when trying to get personal and financial information."
- "This is important. I depend on my hardware vendor to have my computer set up to keep these things updated automatically via internet."

7. Inventory tracking and media controls

"Assemble an inventory of the hardware in use and list the serial numbers. A copy of the inventory is stored off site as this information is important for HIPAA compliance, identification for insurance companies, and tracking theft. The Device and Media Controls standard has 4 implementation specifications: disposal (required), media reuse (required), accountability (addressable), and data backup and storage (addressable). 'Required' indicates that all dental offices that are covered entities must comply with the regulation as written. 'Addressable' indicates that each office can determine how to implement the specification."

Question 1: Does your office maintain an inventory of your hardware with serial numbers, including an off-site copy?
Yes: 38% (6 of 16)
No: 63% (10)

Question 2: If no, do you intend to update your inventory and keep offsite records?
Yes: 50% (5 of 10)
No: 50% (5)

Question 3: If you are not implementing this policy at this time, why not?

- "Again, we're contracted with a company from whom we've purchased all hardware and software, they have records."

- "Not going to bother with it."
- "All records are written. No Computer."
- "Not aware of this yet"
- "Have not been forced to yet"
- "Time consuming and not always practical, daily record copies are kept off site though."
- "I am implementing this only if my vendor is keeping these records."

8. Disposal of hardware and media

"The dental office should have policies and procedures regarding the disposal of hardware and electronic media that contain ePHI. For example, if a practice upgrades their hardware and the old computers are removed from the facility, the hard drives should be erased or destroyed."

Question 1: Do you have a disposal policy?
Yes: 63% (10 of 16)
No: 38% (6)

Question 2: If no, do you intend to implement a policy?
Yes: 50% (3 of 6)
No: 33% (2)
No answer: 17% (1)

Question 3: If you are not implementing a disposal policy at this time, why not?

- "No computer."
- "I would destroy the hard drive myself or store it in the closet."
- "We have done this, it is just not written down."
- "I erase what is stored on the computer."

9. Tracking hardware and media

"Standard CFR 164.310 (d)(2)(iii) specifies that where it is reasonable and appropriate, the covered entity should 'maintain a record of the movements of hardware and electronic media and any person responsible therefore.' This standard requires the security officer to track the movements of hardware and electronic media that contains ePHI.1(p12)"

Question 1: Does your practice have a designated security officer?
Yes: 44% (7 of 16)
No: 56% (9)

Question 2: If no, do you intend to assign this position?
Yes: 22% (2 of 9)
No: 78% (7)

Question 3: How would you rank the importance of an assigned security officer?
Average rank: 1.2

Question 4: Do you or someone else in your office track movements of hardware and media?
Yes: 44% (7 of 16)
No: 56% (9)

Question 5: If No, do you intend to track movement in the future?
Yes: 25% (2 of 8)

No: 63% (5)
No answer: 13% (1)

Question 6: In your words, how important is a security officer to your practice?
"Non-existent"

- "Someone needs to be paying attention, but in a small office it's like having a General with only 3 privates."
- "Not applicable, small practice."
- "All records in my office are written. Without a computer no tracking is needed."
- "Not real critical unless staff is taking computers home to finish up work."
- "It is something that you do without being called a security officer."
- "Somewhat important"
- "Reasonable and appropriate are the key words."
- "Not that important."

10. NPP forms and usage

The following recommendation from the U. S. Department of Health and Human Services concerns the Notice of Privacy Practices (NPP) which dental patients are asked to sign at their first visit. The title of the article is "Protecting the Privacy of Patients' Health Information," which was released in April 2003 (http://www.hhs.gov/news/facts/privacy.html).

"Notice of Privacy Practices"
Covered health plans, doctors and other health care providers must provide a notice to their patients how they may use personal medical information and their rights under the new privacy regulation. Doctors, hospitals and other direct-care providers generally will provide the notice on the patient's first visit following the April 14, 2003, compliance date and upon request. Patients generally will be asked to sign, initial or otherwise acknowledge that they received this notice…. Patients also may ask covered entities to restrict the use or disclosure of their information beyond the practices included in the notice, but the covered entities would not have to agree to the changes."

Question 1: Does your practice request new patients to sign NPP forms?
Yes: 71% (12 of 17)
No: 29% (5)

Question 2: If no, do you intend to adopt the practice?
Yes: 0% (0 of 5)
No: 100% (5)

Question 3: How would you rank the importance of the NPP form?
Average rank: 1.2

Question 4: If you do not present new patients with NPP forms, why not?

- "We do, but they are meaningless. It's the electronic clearinghouses and insurance companies' people we need to worry about."
- "I am not a HIPAA covered entity."
- "The NPP form is presented to every new patient ... some are suspect in signing anything ... I am sure that patients do not feel any more secure in their personal information by signing a document ... we are bound by confidentiality and conduct ourselves appropriately ... this form is only necessary as to the Rule by which dentists must comply."
- "All records are written. Without a computer we have no electronic transfer of information."
- "I am not a covered entity, in my opinion as I don't send Patient info electronically and have no internet at the office."
- "We try to comply, however many times I feel every government agency in the country wants to run my practice without regard to the problems, expense or aggravation it causes the health provider...Gerald W. Daniel D.D.S."

Discussion

Are dentists HIPAA compliant?

If the nine requirements described by HIPAA consultant Olivia Wann; as well as the NPP requirement as stated by HHS are legitimate, then the answer is no. Not a single one of the dentists surveyed is 100% compliant. After all, for requirement number 4, which concerned the security of computer workstations, not one of the 18 answered that their practice had a written workstation policy, which is considered necessary by Ms. Wann.

Compliancy ranged from 0% compliant for workstation policy to 88% compliancy for password security, with an average of 49%. Considering that there were a couple of dentists in the group who do not use computers in their practices, it is safe to say that 100% of the covered entities in this survey use passwords. Password security was also the highest ranked of the requirements: 2.0 on a scale of 0 – 3. Workstation policy was the lowest ranked at 1.1. This shows that if dentists think the requirements make sense, they are more likely to obey the Rule.

There is an interesting clue about dentists' perception of the importance of password security that is revealed by a statistical rarity that is perhaps statistically significant: The standard deviation of the dentists' 16 responses is 1.0. That is highly unusual using such a limited scale of 0 - 3. What it reflects is this: The responses to this question of rank were exclusively 1s and 3s, 8 each, with an average of 2. Here is what the sequence looks like: 1313131131133313. What it means, I don't know. Perhaps it is an indication of an all-or-nothing (much) attitude towards password security that is prevalent in dentists' practices.

Are the requirements a burden on dentists?

From the responses in this study, one can argue that dentists often strive to comply with regulations even though they recognize them as of little value. A good example of this respect of authority is evident in the responses to requirement number 3, "Maintenance documentation." According to the answers provided in the survey, only 3 dentists out of the 17 respondents document maintenance on their computers. Of the 13 who do not document, almost half (6) intend to start, even though the group ranks the importance of such an effort as vey low (1.5 on a scale of 0 to 3).

Nevertheless, there are several disparaging comments reflecting how the Rule fails to take into consideration the small size of dental practices compared to other providers for which it was designed: "No windows, one door, no pipes near computer or backup discs, only one office person uses computer" (1 Contingency plan), "Feel it is not needed" (2 Facility security), "I would destroy the hard drive myself or store it in the closet" (8 Disposal of hardware). The 9th requirement listed which concerns tracking of hardware and assigning a security officer seemed to draw the most comments reflecting a poor fit of the Rule to dental practices: "Non-existent [importance]." "Someone needs to be paying attention, but in a small office it's like having a General with only 3 privates." "Not applicable, small practice."

However, there was one dentist who proclaimed that having a security officer is "extremely important"

There are signs of growing frustration, such as in answers like: "Have not been forced to, yet" (3 Maintenance documentation and 7 Inventory tracking), "Excessive paper work" (3 Maintenance documentation), "... this [NPP] form is only necessary as to the Rule by which dentists must comply" (10 NPP forms and usage) and "Not going to bother with it" (7 Inventory tracking).
Although I made the decision not to include his comments in the results as a matter of decorum, there was also one dentist who repeatedly claimed that he is "Too lazy" to comply. One would be mistaken to take those words at face value. His statement is a pure sign of open defiance, not laziness.

Dr. Gerald Daniel seems to have captured many of the dentists' feelings about the HIPAA Rule when he lamented, "We try to comply, however, many times I feel every government agency in the country wants to run my practice without regard to the problems, expense or aggravation it causes the health provider" (10 NPP forms and usage).

Some of the responses reflect lack of information about the HIPAA requirements. There were comments such as: "We don't know how" (twice: 1 Contingency plan, 2 Facility security) and "Not aware of this" (7 Inventory tracking).

From answers such as "I am not a HIPAA covered entity" and "All records are written. No Computer," it is becoming increasingly evident that dentists who are not covered-entities assume fewer business liabilities than those who transmit patient information digitally.

Do the requirements achieve their intended purposes?

Considering the negative responses to the NPP requirement and its rank of 1.2 (second lowest), one has to wonder why so many of the dentists comply with it (71%). Does a signature on a NPP form make any difference? How could it? Here is the last sentence in the requirement: "Patients also may ask covered entities to restrict the use or disclosure of their information beyond the practices included in the notice, but the covered entities would not have to agree to the changes."

Conclusion

According to this study, it is clear that the HIPAA Rule, as it is presently written, is ill-suited for some dental practices in the nation. If the results from this small sample are indicative of dental practices in general, the enforcement of the HIPAA mandate in the nation's dental practices should be reconsidered.

THE END

www.HealthcareFinancials.wordpress.com