

# The HIPAA Rule and Dentistry:

## A Survey of Dentists – a pilot study. By Darrell Pruitt D.D.S.

Abstract

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

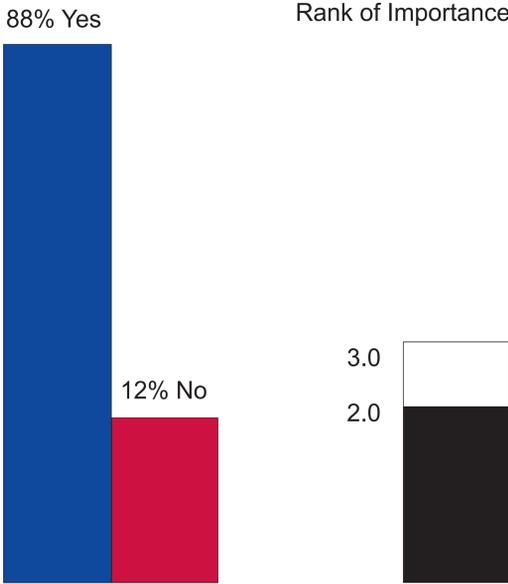
The range of compliancy was found to be from 0% for the requirement of a written workstation policy to 88% for that of password security. The average was 49%, meaning that less than half of the requirements are being respected by the dentists in this sample.

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 needs to be performed before enforcement of the HIPAA mandate is considered for the nation's dental practices.

### 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." Olivia Wann, HIPAA consultant

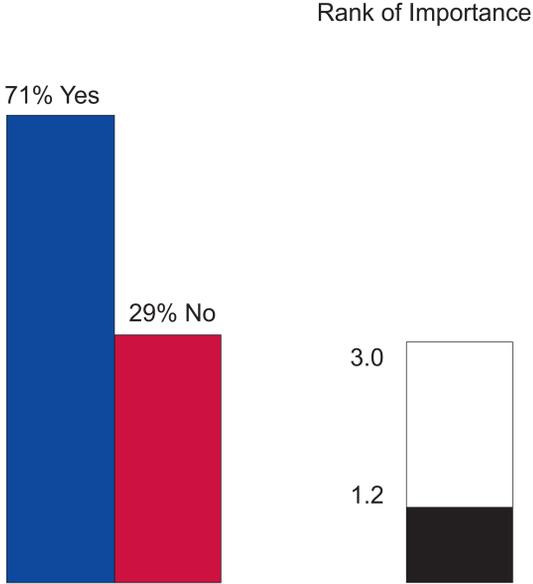
**Question:** Does your practice use passwords?



### 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." - CMS

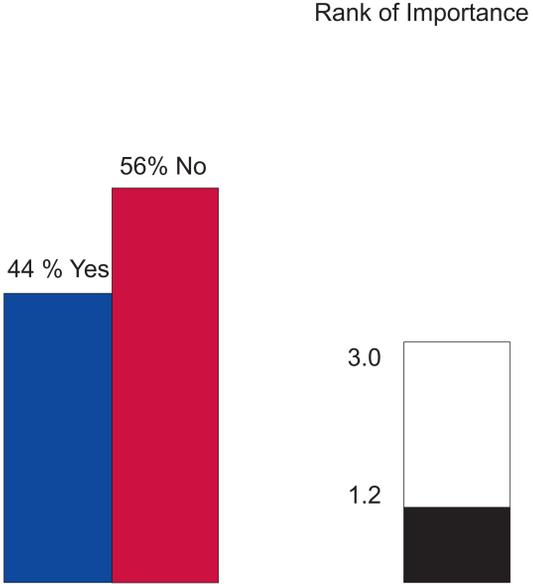
**Question:** Does your practice request new patients to sign NPP forms?



### 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)" Olivia Wann, HIPAA consultant

**Question:** Does your practice have a designated security officer?

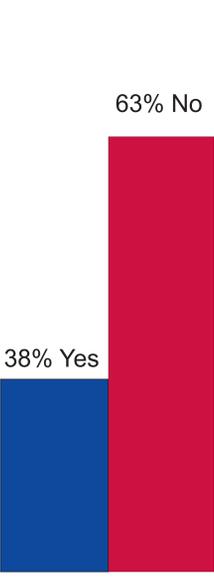


**Question:** In your words, how important is a security officer to your practice?  
 "Someone needs to be paying attention, but in a small office it's like having a General with only 3 privates."  
 "Not applicable, small practice."

### 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." Olivia Wann, HIPAA consultant

**Question:** Does your office maintain an inventory of your hardware with serial numbers, including an off-site



**Question:** If you are not implementing this policy at this time, why not?  
 "Time consuming and not always practical, daily record copies are kept off site though."  
 "All records are written. No Computer."

### Use of Computer Workstations

"The dental office's policy should detail the appropriate use of computer workstations, regardless of where they are located. Operator 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." Olivia Wann, HIPAA consultant

**Question:** Does your practice have a written workstation policy?

