



HIPAA Security Rule FAQ

1. What is this “Security Rule”? Isn’t it the same thing as Privacy? Wasn’t Privacy all of HIPAA?

The HIPAA Security Rule is a separate, distinct regulation which was required by the original 1996 HIPAA legislation. The final version of the Security Rule was published in February 2003 after a lengthy development. The enforcement deadline for the HIPAA Security Rule was April 20, 2005.

2. Do I have to comply with it/does my office need the HIPAA Security Kit?

All of the HIPAA Rules for Privacy, Security, Transactions, and Identifiers apply to a dentist IF the dentist electronically transmits or receives a patient’s protected health information using one of the standard transactions established by the U.S. Department of Health and Human Services.

HIPAA standard transactions are:

Claims or equivalent encounter
Claim attachments
Claim status inquiry
Eligibility Inquiry
Payment Advice or Remittance Advice
Coordination of Benefits/Explanation of Benefits
First Report of Injury for Workman’s Compensation
Enrollment or Disenrollment in a Health Plan
Notice of Premium Payment

For assistance in determining whether you are a covered entity, you may wish to consult the “**Covered Entity Decision Tool**” posted at

<http://www.cms.hhs.gov/hipaa/hipaa2>.

Dentists should note that they will be required to comply with HIPAA even if they indirectly transmit or receive patients’ protected health information using one of the standard electronic transactions. For example, if a dentist sends paper claims to a clearinghouse, which then converts the paper claims to electronic claims and transmits them to a health plan, the dentist is a covered entity.

Keep in mind that faxes are not considered to be electronic transactions because they exist on paper before transmission.

Finally, remember that Dentists who are subject to HIPAA must comply with the Security Rule **in addition to** the Privacy Rule.

3. Who will enforce this rule?

The Centers for Medicare and Medicaid Services’ Office of HIPAA Standards.



3a. We don't see Medicare patients, why are they involved?

CMS is part of the U.S. Department of Health and Human Services, and was named by the Secretary of Health and Human Services to enforce HIPAA rules for Transactions, Security, and Identifiers.

4. It's already past the April 20, 2005 deadline for Security Compliance. I just found out that this new rule existed. Am I in trouble?

If you are a covered entity, it would be very wise to implement the Security Rule as soon as possible. However, there is probably no need to panic. At this time, the Office for HIPAA Standards has no plans to perform random audits and is relying on complaints to drive HIPAA security enforcement. We can not say that this will always be the case. Of course,.

5. What software do I need to comply with this Security Rule?

The Security Rule does not prescribe specific software or technologies; instead, covered providers are given the flexibility to determine whether new security software or devices are needed, based on the practice's actual risks, size, complexity, technical capabilities, and resources.

6. What are some of the main differences between Privacy and Security?

Unlike the Privacy Rule, the Security Rule does not establish any new patient rights. It does not require providers to ask patients to read or sign any forms. The Privacy Rule establishes protections for health information in oral, written, and electronic form. The Security Rule establishes highly detailed standards for the protection of electronic health information, but does not apply to written or oral communications.

The Security Rule requires covered providers to protect the integrity and availability of electronic health information as well as its confidentiality. This means that a) only authorized individuals may access electronic health information (confidentiality), b) that the information does not change except when changed by an authorized person (integrity), and c) authorized persons can always retrieve electronic health information regardless of circumstances (availability).

The Security Rule is composed of Administrative, Physical, and Technical standards. These standards are designed to help protect the confidentiality, integrity, and availability of electronic health information. Covered providers meet these very flexible standards by assessing risks, deciding how to manage risks in a reasonable manner, and documenting their decisions. Ultimately, while the Security rule at first may seem narrower than privacy because it covers only electronic communications, it can cut across even more operational lines, involve more business decisions, and take more time to comply than did Privacy.

7. I use X billing software with Y clearinghouse, they say they're HIPAA compliant, does that mean I'm OK?

Maybe. It is possible that your existing policies, procedures, and safeguards, in combination with your vendors' efforts, could meet HIPAA Security standards without modification. However, there is no way of knowing this for certain without doing a risk analysis. The risk analysis process helps a practice identify and correct its weaknesses.



American Dental Association
www.ada.org

8. What is a Security Officer?

Covered dentists must appoint a Security Official to carry out a risk analysis in order to identify vulnerabilities. After assessing vulnerabilities, the Security Official will write policy or implement safeguards to manage the risks associated with the vulnerabilities. The Security Official will also document existing policy or safeguards that appear to meet Security Rule standards.

The combination of existing and new policy or safeguards forms the practice's Security documentation. In the unlikely event a practice were audited by CMS for Security reasons, this security documentation will help the practice avoid or reduce fines.

9. Who should be my office's Security Official? Can the responsibilities be delegated to an office manager, hygienist, or other staffer?

The Security Rule's standards cut across many practice operations in such a manner that dentists may not feel comfortable with leaving some of the decisions in the hands of an employee. In many cases, the best individual for the job of Security Official may well be the dentist. The job may be delegated, in which case the dentist should keep in mind s/he, as the covered entity, is ultimately responsible for HIPAA compliance.

10. How does the Security Official do the risk analysis? How is it documented?

The ADA HIPAA Security Kit comes with a detailed risk analysis tool (pages 26-34). This tool is a checklist of potential threats and vulnerabilities; answering the questions contained in the tool helps to provide a clearer image of the practice's weaknesses and helps to prioritize implementation activities. The use of this particular checklist is not required; the office must, however, carefully analyze all of the risks in the areas specified by HIPAA.

Documentation of the risk analysis is up to the covered entity, there is no prescribed method. It could be as simple as a log sheet that records the dates of periodic risk assessments.

11. How does one obtain a HIPAA Security Kit?

The ADA HIPAA Security Kit is a useful tool designed to help dentists comply with the HIPAA Security Rule. If you are subject to HIPAA and have not implemented the Security Rule yet, contact the ADA catalog at 800 947-4746, or visit the ADA catalog online at www.adacatalog.org, to order your HIPAA Security Kit today. Cost is \$99.95 for members.