HIPAA Privacy, Security & The Final Omnibus Rule:

What’s New & What Do I Have To Do?

Presented by Leslie Canham, CDA, RDA
Certified Speaking Professional

In the dental field since 1972, helping dental practices simplify complex regulations, she provides in-office training, consulting, workshops, and mock inspections. For the 4th year in a row, she has been listed as a “Leader In Consulting” by Dentistry Today. She is authorized by the Department of Labor, The Academy of General Dentistry, and the California Dental Board to provide continuing education. Leslie is the founder of Leslie Canham and Associates.

This program sponsored by

![CareCredit](https://example.com/carecredit.png)

Making care possible...today.

Leslie Canham CDA, RDA
Speaker, Consultant, Trainer
Action required….New HIPAA Regulations effective in 2013
Have you completed the required tasks?

In January 2013, the new HIPAA Omnibus Final Rules were published implementing changes to HIPAA Privacy, Security, Breach Notification and Enforcement Rules. The deadline for all covered entities to revise their written policies and procedures was September 23, 2013.

Here are some of the things you need to do:

1. Appoint a Privacy/Security Official
2. Conduct and document a “Risk Assessment”
3. Update your Business Associates Agreements and have each business associate sign the new agreement.
4. Re-write and post your HIPAA Notice of Privacy Practices
5. Create new written plans and policies to demonstrate how your practice will adhere to HIPAA regulations.
6. Understand your patient’s rights
7. Train your workforce on the new regulations.
8. Understand how to prevent breaches and know when you must provide breach notification.
9. Create the required Logs:
   - Amendment Request Log
   - Disclosures of Patient Information Log
   - Complaint Log
   - Breach Log
   - Security Incident Log
   - Emergency Access Log
   - Maintenance Repair Log
   - Electronic Media and Hardware Movement Log
10. Have a Disaster Recovery Plan

Resource: The American Dental Association (ADA) 2013 “Complete HIPAA Compliance Kit”. [http://www.ada.org/8833.aspx](http://www.ada.org/8833.aspx) If you have previous versions of the ADA HIPAA privacy and security kits, they are likely outdated. You might be entitled to the upgrade if your HIPAA Kit was purchased in 2011 or 2012. Contact ADA to find out.
"HIPAA", is an acronym for the Health Insurance Portability and Accountability Act of 1996. The HIPAA rule includes a section called Administrative Simplification which is composed of four parts: Privacy Rule, Standards for Electronic Transactions, Unique Identifier Standards, and the Security Rule.

In 2009- HITECH Act Enacted - Breach Notification Rule
In 2013- Final Omnibus Rules

Key provisions of the Privacy Rule include:

- Access to medical records
- Notice of Privacy Practices
- Limits on Use of Protected Health Information
- Confidential Communications
- Complaints
- Written Privacy Policies
- Employee Training
- Privacy Officer

Privacy Official’s responsibilities:

- Develop and implement privacy policies and procedures
- Receive complaints
- Provide further information about matters covered in Notice of Privacy Practices
- Consult/train workforce in all privacy matters
- Document and maintain all policies, procedures and actions taken by the practice with regards to the HIPAA Privacy Rule.

   Retain documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

Create Required Logs:
- Amendment Request Log
- Disclosures of Patient Information Log
- Complaint Log
- Breach Log
- Security Incident Log
- Emergency Access Log
- Maintenance Repair Log
- Electronic Media and Hardware Movement Log
Standards for Electronic Transactions

Unique Identifiers Standards
National Provider Identifier (NPI)  www.nppes.cms.hhs.gov.

Security Rule

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) the Dentist creates, receives, maintains, or transmits.

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.

3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule.

4. Ensure that employees comply with HIPAA.

The Security standards require Dentists to protect ePHI using these safeguards:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

The Security Rule Implementation Specifications are standards that are considered either: Required or Addressable. Required means must be implemented. Addressable means you determine if the standard is reasonable and appropriate for your practice implement the security specification. If not reasonable and appropriate, implement an alternative that is reasonable and appropriate. If there is no reasonable and appropriate alternative, do nothing except document your decision.

Security Official’s responsibilities:

1. Conduct a Risk Assessment to determine if the ePHI is vulnerable.
2. Determine if security has been compromised.
3. Conduct employee training on physical and technical security
4. Enforce security policies
5. Maintain Passwords
6. Oversee and audit failed Log-In attempts
7. Install current firewalls and virus protection, secure computers from theft, keep inventory of computer equipment, back up data in a secure location, and set up a disaster recovery plan.

To utilize an online training game go to:

http://www.healthit.gov/providers-professionals/privacy-security-training-games

For a risk assessment Tool go to:

http://www.healthit.gov/providers-professionals/security-risk-assessment
The HITECH ACT & BREACH NOTIFICATION

In 2009, The Health Information Technology for Economic and Clinical Health Act (HITECH Act) provisions were enacted as part of the American Recovery and Reinvestment Act of 2009. The HITECH Act introduced the new Breach Notification Rule.

According to the Health and Human Services, Office of Civil Rights (OCR), the definition of a Breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of a “breach”.

1. **Unintentional Acquisition**—meaning access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate. Business associates are those who have access to a patient’s protected health information such as an accountant, attorney, consultant, and computer support technicians.

2. **Inadvertent Disclosure**—means inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at a covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

3. The final exception to the breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Covered entities must notify individuals whose personal information was breached. A breach is unauthorized access or use of unencrypted, computerized protected health information. Unauthorized access or use of protected health information on paper, film or other non computer medium also constitutes a breach. A breach of protected health information occurs when the information accessed has a person’s name in combination with any of the following:

- Social Security number,
- Driver’s License or Identification,
- Financial Account number, credit or debit card number,
- Medical Information,
- Health Insurance information
In the event a patient’s unsecured protected health information is acquired, accessed, used or disclosed in an unauthorized way, notification must be made.

1. Patients must be notified without delay but no later than 60 days after discovery of the breach.
2. If the breach affects 500 or more patients, it must be reported to the Department of Health and Human Services and in California, the State Attorney General’s office.
3. If the breach affects 500 or more patients residing in the same area, the breach must be reported to local media and Department of Health and Human Services.
4. Business Associates are now required to notify the dentist if a breach occurs so notifications can be made.

Final HIPAA Omnibus Rule Issued 1-17-13 Effective 3-26-13

Extends patient privacy and security protections under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Final Rule:

- Enhances HIPAA enforcement
- Expands many HIPAA requirements to "business associates" such as contractors and subcontractors that receive protected health information
- Restricts disclosures to a health plan concerning treatment for which the provider has been paid out of pocket in full.
- Modifies rules that apply to marketing and fundraising communications and the sale of protected health information.
- Expands the definition of "health information" to include genetic information.
- Clarifies when data breaches must be reported to the HHS Office for Civil Rights.

Omnibus Final Rule Deadlines 9-23-13

- Business Associates Agreements-must be modified, in writing, and signed
- Notice of Privacy Practices must be revised and re-posted
- Update workforce training on the Final Rule

For more information visit the United States Department of Health and Human Services website at www.hhs.gov.