LESLIE CANHAM
& ASSOCIATES

You Can Think Your Practice is in Compliance….
or You Can KNOW IT!

PO Box 542
Copperopolis, CA 95228
888.853.7543 toll free
209.785.4458 fax
Leslie@LeslieCanham.com
www.LeslieCanham.com

Leslie Canham CDA, RDA
Speaker, Consultant, Trainer

LESLIE CANHAM & ASSOCIATES

Keeping your Practice, Patients and Team as Safe as can Be!

Mock Inspections

Leslie and her husband Mike will conduct a complete inspection of your office. All areas that are not OSHA compliant will be noted in writing and accompanied by suggestions to achieve compliance. Get the help you need to be prepared for OSHA, the Dental Board, or insurance company inspections.

In Office Training

In-office training on "OSHA", "Infection Control", "Dental Practice Act" and "HIPAA". Leslie is a Registered Provider of Continuing Education in California. Earn CE units right in your own office for something you have to do anyway! Mock Inspections are included with in-office OSHA training.

8 Hour Infection Control Course for Unlicensed Dental Assistants

Required training for unlicensed DAs hired after 1-1-10. The didactic portion of the course (4 hours) may be taken as home study. The clinical portion of the course (4 hours) must be presented live, hands-on in a clinical setting. For your convenience, Leslie will conduct the clinical portion of the course in your office. Prefer an 8 hour live course completed in one day? Leslie will accommodate.

Consulting

Need help getting your OSHA, MSDS or HIPAA programs started? Leslie will come to your office and help you get the required manuals, record-keeping forms and paperwork organized. Leslie will walk you through the mandatory requirements so you can achieve compliance. Telephone consulting is also available at $95 per 20 minutes. First 10 minutes are no charge!

Manuals and Training DVDs

- ***Employee OSHA Check List and Training Record Binder*** **$55**
  Includes training records and new employee orientation checklist for OSHA compliance.
- ***Exposure Incident Binder*** **$55**
  Helps to expedite and streamline the process and forms that must be gathered when an employee needs medical attention for an exposure incident.
- ***OSHA-Annual Bloodborne Pathogen Training DVD and Workbook*** **$499**
  (Includes Employee OSHA and Exposure Incident Binders)
  Employees watch the DVD and fill out the forms. This the easiest way for Dentists to provide the required OSHA training.

Online Home Study Courses and Webinars*

Dental Practice Act, Infection Control, OSHA, HIPAA, MRSA, Safe Dental Care, and more.
*Webinars are live courses taken from your computer. Webinars count as live classroom credit!

About Leslie

Leslie Canham is a Certified and Registered Dental Assistant with over 39 years of experience in dentistry. As a past president of the San Fernando Valley Dental Assistants Society, she has participated in numerous continuing dental education seminars. Leslie speaks to dental societies and organizations as well as being the moderator of the Infection Control Forum on Dentaltown.com. Leslie's articles and home study courses appear in numerous dental publications. She is authorized by the Department of Labor as an OSHA Outreach Trainer in General Industry Standards. Her professional organization memberships include: The California Association of Dental Assistant Teachers, the Organization for Safety, Asepsis and Prevention, The Speaking, Consulting Network, the Academy of Dental Management Consultants, the National Speakers Association, the California Dental Assistants and California Dental Associations. Leslie is a registered provider of continuing education with the California Dental Board.

Contact Leslie- 888-853-7543 or online LeslieCanham.com

P.O. Box 542 Copperopolis, CA 95228 Phone: 209-785-3903 Fax: 209-785-4458
email: Leslie@LeslieCanham.com Web: LeslieCanham.com

HIPAA

"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:

1. Privacy Rule
2. Standards for Electronic Transactions
3. Unique Identifiers Standards
4. Security Rule

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 with 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 <u>six years from the date of its creation or the date when it last was in effect, whichever is later.</u>**

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

The HITECH ACT

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, or
Driver’s License or Identification, or
Financial Account number, credit or debit card number, or
Medical Information, or
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 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 .

HIPAA Compliance 2013

Here are some of the things you need to do:

1. Conduct and document a “Risk Assessment”
2. Re-write your current HIPAA Notice of Privacy Practices.
3. Update your Business Associates Agreements and have each business associate sign the new agreement.
4. Create new written plans to demonstrate how the practice will adhere to HIPAA regulations.
5. Train your workforce on the new regulations.
6. Understand how to prevent breaches and know when you must provide breach notification.
7. 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

While all these tasks seem overwhelming, you don’t have to invent all the written forms and logs. I highly recommend that your practice purchase the American Dental Association (ADA) “Complete HIPAA Compliance Kit ”. Of all the available HIPAA manuals in the market place, the ADA kit, in my opinion is the best. You may purchase the ADA HIPAA kit (ADA item #: J598) by calling ADA at 800-947-4746 or online on the ADA website using the following link:

http://www.ada.org/8833.aspx

The cost of the kit is currently $300 for ADA members and $450 for non members. 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.

{NAME OF PRACTICE}

Sample Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY. THE PRIVACY OF YOUR HEALTH INFORMATION IS IMPORTANT TO US.

Our Legal Duty

We are required by applicable federal and state law to maintain the privacy of your protected health information. We are also required to give you this Notice about our privacy practices, our legal duties, and your rights concerning your protected health information. We must follow the privacy practices that are described in this Notice while it is in effect. This Notice takes effect ____/____/____, and will remain in effect until we replace it.

We reserve the right to change our privacy practices and the terms of this Notice at any time, provided such changes are permitted by applicable law. We reserve the right to make the changes in our privacy practices and the new terms of our Notice effective for all health information that we maintain, including health information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this Notice and provide the new Notice at our practice location, and we will distribute it upon request.

You may request a copy of our Notice at any time. For more information about our privacy practices, or for additional copies of this Notice, please contact us using the information listed at the end of this Notice.

Your Authorization: In addition to our use of your health information for the following purposes, you may give us written authorization to use your health information or to disclose it to anyone for any purpose. If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures permitted by your authorization while it was in effect. Unless you give us a written authorization, we cannot use or disclose your health information for any reason except those described in this Notice.

Uses and Disclosures of Health Information

We use and disclose health information about you without authorization for the following purposes:

Treatment: We may use or disclose your health information for your treatment. For example, we may disclose your health information to a physician or other healthcare provider providing treatment to you.

Payment: We may use and disclose your health information to obtain payment for services we provide to you. For example, we may send claims to your dental health plan containing certain health information.

Healthcare Operations: We may use and disclose your health information in connection with our healthcare operations. For example, healthcare operations include quality assessment and improvement activities, reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, conducting training programs, accreditation, certification, licensing or credentialing activities.

To You or Your Personal Representative: We must disclose your health information to you, as described in the Patient Rights section of this Notice. We may disclose your health information to your personal representative, but only if you agree that we may do so.

Persons Involved in Care: We may use or disclose health information to notify, or assist in the notification of (including identifying or locating) a family member, your personal representative or another person responsible for your care, of your location, your general condition, or death. If you are present, then prior to use or disclosure of your health information, we will provide you with an opportunity to object to such uses or disclosures. In the event of your absence or incapacity or in emergency circumstances, we will disclose health information based on a determination using our professional judgment disclosing only health information that is directly relevant to the person's involvement in your healthcare. We will also use our professional judgment and our experience with common practice to make reasonable inferences of your best interest in allowing a person to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of health information.

Disaster Relief: We may use or disclose your health information to assist in disaster relief efforts.

Marketing Health-Related Services: We will not use your health information for marketing communications without your written authorization.

Required by Law: We may use or disclose your health information when we are required to do so by law.

Public Health and Public Benefit: We may use or disclose your health information to report abuse, neglect, or domestic violence; to report disease, injury, and vital statistics; to report certain information to the Food and Drug Administration (FDA); to alert someone who may be at risk of contracting or spreading a disease; for health oversight activities; for certain judicial and administrative proceedings; for certain law enforcement purposes; to avert a serious threat to health or safety; and to comply with workers' compensation or similar programs.

Decedents: We may disclose health information about a decedent as authorized or required by law.

National Security: We may disclose to military authorities the health information of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials health information required for lawful intelligence, counterintelligence, and other national security activities. We may disclose to correctional institution or law enforcement official having lawful custody the protected health information of an inmate or patient under certain circumstances.

Appointment Reminders: We may use or disclose your health information to provide you with appointment reminders (such as voicemail messages, postcards, or letters).

Patient Rights

Access: You have the right to look at or get copies of your health information, with limited exceptions. You may request that we provide copies in a format other than photocopies. We will use the format you request unless we cannot practicably do so. You must make a request in writing to obtain access to your health information. You may obtain a form to request access by using the contact information listed at the end of this Notice. You may also request access by sending us a letter to the address at the end of this Notice. We will charge you a reasonable cost-based fee for the cost of supplies and labor of copying. If you request copies, we will charge you $0.___ for each page, $___ per hour for staff time to copy your health information, and postage if you want the copies mailed to you. If you request an alternative format, we will charge a cost-based fee for providing your health information in that format. If you prefer, we will prepare a summary or an explanation of your health information for a fee. Contact us using the information listed at the end of this Notice for a full explanation of our fee structure.

Disclosure Accounting: You have the right to receive a list of instances in which we or our business associates disclosed your health information for purposes other than treatment, payment, healthcare operations, and certain other activities, for the last 6 years, but not before April 14, 2003. If you request this accounting more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests.

Restriction: You have the right to request that we place additional restrictions on our use or disclosure of your health information. In most cases we are not required to agree to these additional restrictions, but if we do, we will abide by our agreement (except in certain circumstances where disclosure is required or permitted, such as an emergency, for public health activities, or when disclosure is required by law). We must comply with a request to restrict the disclosure of protected health information to a health plan for purposes of carrying out payment or health care operations (as defined by HIPAA) if the protected health information pertains solely to a health care item or service for which we have been paid out of pocket in full.

Alternative Communication: You have the right to request that we communicate with you about your health information by alternative means or at alternative locations. (You must make your request in writing.) Your request must specify the alternative means or location, and provide satisfactory explanation of how payments will be handled under the alternative means or location you request.

Amendment: You have the right to request that we amend your health information. Your request must be in writing, and it must explain why the information should be amended. We may deny your request under certain circumstances.

Electronic Notice: You may receive a paper copy of this notice upon request, even if you have agreed to receive this notice electronically on our Web site or by electronic mail (e-mail).

Questions and Complaints

If you want more information about our privacy practices or have questions or concerns, please contact us.

If you are concerned that we may have violated your privacy rights, or you disagree with a decision we made about access to your health information or in response to a request you made to amend or restrict the use or disclosure of your health information or to have us communicate with you by alternative means or at alternative locations, you may complain to us using the contact information listed at the end of this Notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to the privacy of your health information. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Contact Officer: _____

Telephone: _____ Fax: _____

E-mail: _____

Address: _____

Appendix 5-3

Sample Emergency Access Log

Use this form to maintain a log of emergency access activities. Identify when emergency access involved emergency responders, such as the Fire Department, Law Enforcement, or Emergency Rescue. Also, log events that were the result of a workforce member's abusive activity and the sanctions imposed.

Name of Practice _____

Facility Address _____ City _____ State _____ Zip _____

Describe Incident		Who Initiated Access?[1]	Emergency Involved		Abusive Activity		Official[2]
Description	Date		Yes/No	Dept.[3]	Describe	Sanctions	

[1] Identify the person who initiated emergency access procedures.
[2] Security Official or delegated representative acting on the S/O's behalf.
[3] Indicate the emergency responder.

Appendix 2-20

Sample Log of Patient Requests for Accounting of Disclosures of Protected Health Information

This sample form illustrates how a dental practice may log requests from patients for accounting of disclosures of their protected health information records in the practice's designated record sets.

Patient Name	Chart/ID Number	Date of Disclosure	Description of PROTECTED HEALTH INFORMATION Disclosed	Purpose of Disclosure	To Whom Disclosure Made

Appendix 4-9
Sample Security Incident Log

Date	Location	Description	Severity Level of Incident 1: Least Serious 5: Most Serious
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5
			1 2 3 4 5

Appendix 2-16
Sample Access Request Log

This sample form illustrates how a dental practice may document its response to patients' requests for access to their protected health information records in the practice's designated record sets.

Name of Practice _____

Patient Name	Chart/ID Number	Date of Review	Reason for Access	Response to Request	Date Patient Notified

Appendix 2-6

Sample HHS Access and Disclosure Log

This sample form illustrates how a dental practice could document access and disclosure of protected health information (PHI) in response to a Department of Health and Human Services (HHS) compliance audit or complaint investigation.

Patient Name	Chart/ID Number	Date of Disclosure	HHS Representative Receiving Disclosure	Description of PHI Disclosed	Purpose of Disclosure

Appendix 2-23
Sample HIPAA Privacy Complaint Log

This sample form illustrates how a dental practice may log HIPAA Privacy or Security Complaints received by the practice from or on behalf of patients or by patients' authorized representatives, or from the Department of Health and Human Services as part of a complaint investigation.

Complaint	Patient or Personal Representative Filing Complaint	Date Complaint Reviewed and by Whom	Date Response Sent to Patient	Sanctions, if Any	Practice-Wide System Changes, i.e. Training, Process Redesign

Appendix 2.22.2
Sample Breach Log

This sample form illustrates how a dental practice might log breaches that affect less than 500 individuals for annual submission to the U.S. Department of Health and Human Services. The following information must be recorded for every breach of unsecured patient information.

Date of breach: _____

Date breach was discovered: _____

Did the breach occur at or by a business associate?

- ☐ Yes
- ☐ No

If yes:

Name of business associate: _____

Address: _____

City: _____ State: _____ Zip code: _____

Business associate contact name: _____

Business associate contact phone number: _____

Business associate contact email: _____

Approximate number of individuals affected by the breach: _____

Type of breach:

- ☐ Theft
- ☐ Loss
- ☐ Improper disposal
- ☐ Unauthorized access or disclosure
- ☐ Hacking or information technology incident
- ☐ Unknown
- ☐ Other: _____

Where was the breached information located?

- ☐ Laptop
- ☐ Desktop computer
- ☐ Network server
- ☐ Email
- ☐ Other portable electronic device
- ☐ Other
- ☐ Electronic medical record
- ☐ Paper

Type of patient information involved:

- ☐ Demographic information
  - o Name
  - o Social Security number
  - o Address or zip code
  - o Driver's license number
  - o Date of birth
  - o Other identifier
- ☐ Financial information
  - o Credit card or bank account number
  - o Claims information
  - o Other financial information
- ☐ Clinical information
  - o Diagnosis or conditions
  - o Lab results
  - o Medications
  - o Other treatment information
- ☐ Other

Brief Description of the breach (include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and type of protected health information involved in the breach):

_____

_____

_____

What safeguards (protective measures) were in place prior to the breach:

- ☐ Firewalls
- ☐ Packet filtering (router-based)
- ☐ Secure browser sessions
- ☐ Strong authentication
- ☐ Encrypted wireless
- ☐ Physical security
- ☐ Logical access control
- ☐ Anti-virus software
- ☐ Intrusion detection
- ☐ Biometrics

Date(s) notice was provided to affected individual(s):

Date first notice was sent:

Month: _____ Day: _____ Year: _____

Date last notice sent:

Month: _____ Day: _____ Year: _____

Was substitute notice required? (Substitute notice is required if you lack sufficient or up-to-date contact information for any affected individuals)

☐ Yes

☐ No

Was media notice required? (Media notice is required if a breach involves 501 or more residents of a state or jurisdiction)

☐ Yes

☐ No

What action did the dental practice take in response to the breach?

☐ Security and/or privacy safeguards

☐ Mitigation (actions to lessen the harm of the breach to affected individuals)

☐ Sanctions (against workforce members who violated the policies and procedures)

☐ Policies and procedures

☐ Other

If "other," please describe: _____

Describe in detail any additional actions taken following the breach:

_____

_____

_____

_____

This form provides for the recording of the information required by the Office for Civil Rights ("OCR") when submitting reports of breaches. See OCR, *Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information http://ocrnotifications.hhs.gov.* **This material is for general reference purposes only and does not constitute legal advice. It covers only HIPAA, not other federal nor state law. Changes in applicable laws or regulations may require revision. Dentists should contact qualified legal counsel for legal advice, including advice pertaining to HIPAA compliance, the HITECH Act, and the U.S. Department of Health and Human Services rules and regulations.**

You Can Think Your Practice is in Compliance… or You Can KNOW IT!

Speaker Leslie Canham, CDA, RDA

Required Posters, Signs and Notices

Notice to Consumers: Dental Board, Dental Hygiene Committee, Consumer Affairs
Prop 65 Amalgam and Nitrous Oxide
Dental Material Fact Sheet
Employment Posters
Dental Board Posters
Radiation Safety Posters
Laser Signs
OSHA Signs

OSHA

OSHA has designed a new, standardized format for Safety Data Sheets (SDS) formerly called Material Safety Data Sheets (MSDS). The SDS will have 16 specific sections designed to ensure consistency across industries and nations. Employers must train their workers in the new label and data sheet requirements by December 1, 2013. This course will provide you with the tools needed to conduct this training.

Review of what OSHA Training/Recordkeeping forms are required.

Discussion of Aerosol Transmissible Diseases" (ATDs), employee training requirements and what written plans addressing ATDs must be part of the office OSHA manual.

Conduct Your Own Mock Inspection- Receive "How to Pass an OSHA Inspection Checklist"

Minimum Standards for Infection Control

What written protocols/posters are required
What's coming our way with new CDC Guidelines