Blood, Spit and Fears

Instructor: Laney Kay, JD

Contact information:
PO Box 71385
Marietta, GA 30007-1385
770-312-6257 (*phone*)
(770) 998-9204 (*fax*)
laney@laneykay.com
www.laneykay.com

OFFICIAL DISCLAIMER
from Laney Kay
Entertaining Training, LLC.
(*now necessary because someone pitched an absolute hissy fit)*:

This program is intended to fulfill the annual training requirements of OSHA's Bloodborne Pathogens Standard and you will receive continuing education credit. In addition, this program is intended only to offer general guidance regarding bloodborne pathogens, OSHA regulations, HIPAA regulations, hazard communication and other related topics; any suggestions offered by me are only my opinion and should not be construed as advice, legal or otherwise. Any specific questions, circumstances, or situations you are concerned about in your particular office should be addressed by your own attorney. Nothing I say is intended to establish a standard of care or industry custom. No one, including me, can "OSHA-proof" or "HIPAA-proof" an office and nothing said in this program will reduce your likelihood of an OSHA or HIPAA inspection, nor will it prevent you from getting fined, nor will it reduce the amount of the fine in the event of an inspection.

AND NOW FOR THE NOT-AS-OFFICIAL DISCLAIMER...

Any other information is intended for entertainment purposes only, and I'll apologize now in the event you don't find me entertaining. Nothing said is intended to offend you or any attendee, and I apologize if you are offended in any way.

OSHA and INFECTION CONTROL CHECKLIST

CHECKLIST ITEMS	YES	NO	FOLLOWUP
Do you have an OSHA manual? (Is it opened and filled in as needed?)-This includes your written policies, guidelines, and office procedures related to infection control and the OSHA Bloodborne Pathogens Standard.			
Do you have an individual specified as the OSHA officer for the office? (They're in charge of filling out the notebook, arranging for training, maintaining the employee records, etc.)			
Do you have policies for training employees? Employees must be trained: at the time of initial employment; if infection control related procedures or tasks are changed; annually. Training must be appropriate in content, level of education, and language of participants.			
Is all employee training documented and placed in the OSHA manual?			
Does everyone in the office know where the manual is kept?			
Have all employees who work in the back received the Hepatitis B vaccination and testing to confirm immunity (or if they refuse to take it, have they signed a declination form)?			
Are employees aware that current health care guidelines recommend other vaccines for healthcare workers, such as flu shots, measles/mumps/rubella, tetanus/diphtheria/pertussis, etc. and that should consult with their own doctors about taking these vaccinations?			
In the event of a TB exposure, is TB testing provided for employees?			
Do you have policies and procedures in place in the event of an employee stick injury and are all employees aware of the policies and procedures?			
Do employees know to immediately report any injuries, especially stick injuries?			
Do you have a place to send the injured employee and the source patient that will give HIV test results in 24 hours or less?			
Are employees aware of any work restriction policies (such as inability to provide direct patient care with an active staph infection on the hands, health evaluations in the event the employee contracts a disease such Hepatitis B, etc.)?			
Does each employee have a confidential medical record that is kept separate from the rest of the OSHA materials? (Includes HBV vaccine and testing information, info on employee injuries and follow-up, etc.)			
Preventing the Transmission of Bloodborne Pathogens in the Dental Office			
Does everyone use standard precautions when working anywhere in the back (operatories, labs, sterilization area, etc.)? (Standard precautions require us to treat all people, all body fluids, all potentially contaminated materials, as potentially infectious)			
Are work practice controls used to reduce exposure to potentially infectious materials? (Work practice controls change the way we do things to make our procedures safer. For example, use one handed recapping methods, place sharps containers close to where they're used, etc.)			
Are engineering controls used to reduce exposure to potentially infectious materials? (Engineering controls isolate us from hazards, such as personal protective equipment, gloves, sharps containers, safety scalpels, etc.)			
Are new technologies evaluated every year to see if new products could make sharps use safer in your office? (Example: new safety syringes, new IV needles, etc.)			
Do employees perform correct hand hygiene when hands are dirty, if a potentially infectious material is touched with bare hands, before putting on gloves, after removing gloves, and between patients? (Always wash your hands using soap and water when first entering an operatory and/or if hands are visibly soiled; otherwise, hand sanitizers are also fine.)			
Are hand hygiene policies in effect for those who work in the back? (Fake fingernails and large rings aren't a great idea; nails should be relatively short and smoothly filed to prevent snagging gloves, etc.)			

Checklist Items	Yes	No	Follow-up
Do employees know which gloves are to be worn for various purposes? (Examples: surgical gloves for long surgical procedures, exam gloves for regular procedures, utility gloves for processing instruments, etc.)			
Do employees know when to change gloves? (Gloves must be changed if torn/snagged, between patients, and should be removed before leaving an operatory. Never wash gloves.)			
Are employees trained on the different types of materials used for gloves, and when the different types are appropriate? (Use nitrile exam gloves if patient or employee has latex sensitivities, certain chemical exposure may require different glove types, etc.)			
Are different types of gloves and other PPE available in different sizes to accommodate each employee?			
Have employees received training on all forms of personal protective equipment (PPE)?			
Do employees know that personal protective equipment must be worn any time there's exposure to potentially infectious materials?			
Do employees understand that the degree of exposure determines what specific PPE is to be worn? (Example: long sleeves if spatter or aerosol is generated, eye protection, etc.)			
Are procedures and policies in place so that employees know what types of PPE are to be worn in each situation? (Examples: while working on a patient, while working in the lab or sterilization area, while using disinfectants and other chemicals to clean an operatory or other area, while taking x-rays)			
Do employees wears masks and change them between patients (or if they become wet)?			
Is eye protection worn any time there is possible exposure to potentially infectious materials?			
Do employees know to remove PPE before leaving the work area?			
Are jackets/gowns disposed of or laundered at the work site? (Or sent off to be laundered)			
Sterilization and Disinfection of Instruments and other items used to care for patients			
Are all instruments that go into the mouth either heat-sterilized or thrown away? (Exceptions would be instruments such as digital x-ray sensors and digital perio probes that can't be heat sterilized. Follow manufacturers' instructions for disinfection on these instruments.)			
Are cleaning and disinfection procedures in place for instruments that cannot be removed from air/water lines?			
Are handpieces sterilized between uses?			
Is the sterilization area well organized with a clear division between the clean side and the dirty side? (So that you can tell whether an item is clean or dirty just by its location in the area?)			
Are instruments processed the same way every time?			
Do employees wear thick utility gloves, jackets, and eye protection while processing instruments?			
Are instruments cleaned in the ultrasonic to remove any debris and bioburden?			
If handscrubbing is necessary, are procedures in place requiring employees to wear eye protection, use a long handled brush, use utility gloves and handle the instruments carefully to avoid an injury?			
Is the ultrasonic solution changed at least once a day, or if it becomes too contaminated?			
Is the ultrasonic tested regularly as recommended by the manufacturer? (Usually by performing a "foil test' to insure that the machine is functioning properly.)			
Are instruments inspected before packaging?			
Are chemical indicators that change color used on the inside and outside of the packaging to insure that the proper temperatures are reached?			
Are packaged instruments labeled with the date and which sterilizer was used (if the office uses more than one)? This allows instruments to be retrieved if there's a spore test failure.			
If cassettes are used, are an FDA approved wrap used on the outside to prevent contamination?			
Are instruments allowed to cool and dry in the sterilizer before handling?			

Checklist Items	Yes	No	Follow-up
Are procedures in place to follow up after a positive spore test?			
Are procedures in place to make sure implantable devices are properly sterilized and stored?			
Are all instruments wrapped or bagged (even individual instruments)?			
Are sterilizers loaded properly so that instruments can be easily sterilized? (When autoclaves are overloaded, instruments may not be adequately sterilized.)			
Are instruments stored in cabinets, drawers, or shelves? (Don't store them under sinks or any other place they could become wet because the pack sterility may be compromised)			
Before procedures, are packaged instruments opened in front of patients so they can see that they've been sterilized?			
In the operatories, are barriers used on items that are difficult to clean and disinfect?			
Are all barriers changed between patients?			
Are all exposed clinical contact surfaces properly cleaned and then disinfected with a tuberculocidal disinfectant between patients?			
Are the proper cleaners and disinfectants used properly? (Example: glutaraldehyde and other liquid sterilants should never be used to clean a surface or in an ultrasonic tank)			
Is a cleaning schedule in place for all areas in the office? (Sterilization area, walls, floors, etc.)			
Do you use either "spray-wipe-spray" OR "use a wipe to clean-discard the wipe-get another wipe to disinfect" method in order to properly clean and disinfect contaminated surfaces in operatories?			
Are employees trained to use wipes properly? (Keep the container closed between uses so they'll stay wet, use them to clean only the proper amount of surface area, leave the surface wet for the proper amount of time, don't use disinfectant-saturated gauze)			
Are hard surface floorings used in operatories, sterilization area, lab, etc., instead of carpet?			
Are procedures in place to handle extracted teeth? (You CAN give them to patients.)			
Is all of the water that goes into patients' mouths at least drinking water quality, which is 500 cfu/ml of water? (From handpieces, air/water syringe, ultrasonics, etc.)			
Is sterile water used when performing surgical procedures?			
Are policies and procedures in place to contain and properly dispose of medical waste, such as sharps or blood saturated materials? (Be aware that there are both state and federal regulations.)			
Hazard Communication Standard			
Do you have a written Hazard Communication Plan/Program?			
Has a hazard assessment established what hazards are present in the office?			
Have you made a list of all products in your office containing hazardous chemicals?			
Do you have an MSDS (now SDS) notebook for all hazardous chemicals?			
Do all chemicals have labels? (Labels must be made for any chemicals out of their original containers, such as ultrasonic tanks, cold sterile solution, etc.)			
Have all employees received training at the time of original employment, whenever hazards are added or changed in the workplace, and periodically, as needed?			
Have employees received training on the new labeling and SDS forms and requirements of the updated Hazard Communication Standard? (It now uses the Globally Harmonized System of Classification and Labeling of Chemicals?)			
Is all training documented and placed in the OSHA notebook?			

HIPAA Checklist and Risk Assessment

In order to comply with the HIPAA Security Rule, all covered providers must have regular risk assessments to ensure that their patients' private health information is as safe as possible. Although you probably completed a comprehensive risk analysis at the time the HIPAA policies were first implemented, risk assessment is an ongoing process. Here is a sample risk analysis you can use that is based upon a document from HHS designed to help small providers with HIPAA security compliance. We all make changes in our offices that can result in compromising the security of patients' information; regular risk assessments help us ensure that we keep the information as safe as possible.

The standard requires that we regularly assess administrative, technical and physical safeguards to ensure compliance with the HIPAA rules. This form will help you perform regular checks. Please note this is a sample risk analysis that you may use to formulate your own policies and risk assessments, and may not cover every situation that may exist in every office, so always check with your own attorney or malpractice carrier to make sure your assessment is complete.

Please fill out this form. For any actions that need to be performed, number the item, and at the end, fill out the actions that must be taken for each numbered item on the attached action plan.

Administrative Safeguards	Yes	No	Needs to be addressed	Item # on action plan
General office information				
Have you conducted a thorough risk analysis to determine potential risks and vulnerabilities to the safety of patient's electronic private health information (PHI)?				
Do you have a security and/or privacy officer in charge of the HIPAA program? Name(s):				
Do you know where PHI is located in the office? Please underline all that apply: desktop computer , laptop computer, tablets, smartphones, server, flash drive, removable hard drives, CDs, paper charts, other: _____				
Do you have a current inventory of all technical items that may contain patients' PHI?				
Do you know the approximate value of all technical items that may contain patients' PHI?				
Have you taken reasonable security measures to protect your patient's information, including door locks, the use of passwords, security systems, and other measures to ensure that PHI is secured?				
Do you have a current backup in the event of a natural disaster so that your patients' information can be easily restored?				
Do you have control over the information on your computer system?				
Business Associates				
Does any vendor or business associate have access to your computer system?				
Does any vendor or business associate have the ability to access and change confidential patient data? If so, are audit logs monitored to prevent unauthorized access?				
Do you have business associate agreements in place for all vendors who may have access to your patients' PHI?				
Do these agreements have assurances that these business associates will properly protect patients' information?				
Do you use a clearinghouse, and if so, do they take precautions to protect your patients' information during processing and transmission?				
Do these agreements include specifics about who's responsible for breach notification				
Do these agreements include indemnification agreements in the event a breach is caused by a business associate?				

Administrative safeguards (continued)	Yes	No	Needs to be addressed	Item # on action plan
Employee Information				
Have your employees received training on basic HIPAA requirements (Privacy, Security, HITECH, and Omnibus Acts)?				
Do you provide additional training if new policies and procedures are implemented?				
Do you document all employees training?				
Do you have written policies and procedures that explain employee requirements under HIPAA?				
Do you contact references and/or conduct background checks before hiring employees?				
Do employees know where the HIPAA manual is kept?				
Do all employees understand there are specific sanctions for violating HIPAA Privacy and Security policies (including being fired) and that all sanctions will be enforced?				
Do all employees understand that, in addition to workplace sanctions, they can also be fined and imprisoned for deliberately violating HIPAA rules?				
Do only those employees, who need access to patients' PHI, actually have access to PHI? (Those without authorization, should not be able to access patients' information)				
Does each employee have a specific log in ID?				
Do you use passwords on your system to prevent unauthorized access?				
Are employees trained not to share passwords or leave them in places that are easily accessible?				
If you have any employees who are not authorized to access patients' PHI, could they access it?				
Do terminated employees still have access to your computer system or do you have systems in place to prevent that scenario?				
Are locks/passwords/etc. changed to prevent continued facility access after termination?				
Do you periodically review employees' access to PHI as needed? (If they change to a job that no longer requires access to patients' PHI, they should no longer have access)				
If any employees can access your system using their personal devices, are they aware of encryption requirements?				
If any security/privacy lapses among employees occur, is additional training and instruction provided?				
Do new employees receive training about the HIPAA programs and are informed about policies, sanctions, etc.?				
Do employees know to inform the HIPAA officer immediately if they suspect information has been compromised?				
General computer protection information				
Would you know if someone was trying to hack into your system?				
Do you have audit logs that may show unsuccessful log-ins or other indicators of unauthorized access?				
Are passwords protected and changed when indicated?				
In the event of computer destruction or loss, are there policies and procedures to restore computer service and restore data (does everyone know who to call)?				
Do employees know they should not install personal software or access personal e-mails on the office computer system because of the potential for viruses and malware?				
If you offer patients Wi-Fi in your office, is their access on a separate router to prevent access to your system?				
Do you perform regular risk assessments and security evaluations, at least annually or any time a change is made?				

Administrative safeguards (continued)	Yes	No	Needs to be addressed	Item # on action plan
Do you have firewalls, anti-viral software, etc. to protect your information from malware/spyware/viruses? (If you use a computer expert, have him write a summary of precautions you've taken to place in your HIPAA manual)				
Are any security incidents documented?				
Do you backup your data?				
Is your data stored offsite in the event the office is destroyed? (What if your home is destroyed at the same time? You should have data backed up in a manner that will provide for widespread devastation to a large area.)				
Do you have a plan that will allow you to temporarily relocate if your office is damaged?				
In the event you're in a temporary location, could patients' information be adequately protected?				
Do you have copies of existing software in the event you have to replace a computer?				
If you make changes to your computer system or relocate computers in the office, do you evaluate the situation to ensure that the new changes do not compromise security? (For example, you move a computer to a consult room and patients may have unsupervised access in that room; passwords, etc. would be very important on that computer).				
Physical Safeguards				
Is your facility protected from unauthorized physical access? (Do you have door locks, cameras, alarms, physical safeguards preventing computer removal, locked cabinets, etc?)				
If hardware, doors, locks, walls, etc. are repaired or modified, are any changes that could affect the security of PHI should be documented?				
Do you use screen savers, privacy screens, etc. to ensure that patient information isn't easily visible to others?				
Are computers placed to ensure that patients' PHI isn't easily visible to others?				
Are computers placed to ensure that unauthorized people don't have unsupervised access? (And if they are unsupervised, is there adequate protection to ensure that other patients' information can't be accessed?)				
Do unattended computers automatically log off when not being used?				
If computers or electronic media are no longer being used/are being replaced, is there a method that destroys the data before disposal?				
Are all flash drives, hard drives, etc. all accounted for and it is known who has them in their possession at all times?				
Is data consistently backed up?				
If data is backed up to a physical item such as a CD or flash drive, how are they protected, stored and destroyed?				
Technical Safeguards				
Since each employee has a unique identifier in the computer system, could their activities be tracked in the system?				
Are passwords unique and not shared?				
Are employees notified that they may be sanctions if they share passwords or use someone else's identifier?				
Do employees have access to only the minimum PHI necessary to do their job duties? (This is usually not relevant in most dental offices where those who have access need access to everything; however, some larger practices do have separate departments for billing, etc.)				

Technical safeguards (continued)	Yes	No	Needs to be addressed	Item # on action plan
If you have automatic logoff for computers, does the time before it logs off shorten for those computers in high traffic areas?				
Do you use e-mail in the office to transmit PHI?				
Do you have a method to encrypt e-mails if it's used to transmit PHI?				
Are other methods of protecting documents, such as password protection of individual documents, used?				
If a patient requests information and the doctor/employee doesn't have access to the encrypted email address to transmit the information, do the doctor and employees know they can request patient permission to transmit using an unencrypted e-mail and then transmit only if permission is granted?				
Are users denied access after a certain number of failed log-in attempts?				
Does the doctor and/or security officer know how to conduct audits for altered information, failed log-ins, etc.?				
Are charts or electronic devices ever taken out of the office (including backup devices, smart phones, etc.)?				
Is your electronic PHI protected by encrypting your information? (Encryption is the only method that will actually render electronic information "unusable" which can avoid a breach in the event your information is accessed, lost, or stolen.)				
If your information is not encrypted, do you have encrypted passwords?				
Are any electronic portable devices that can access patients' information encrypted?				
Do your employees know to immediately report any suspected breaches of information?				
Do your business associates know to immediately report any suspected breaches of information and provide you with all needed information to determine if a breach has occurred?				
Do your business associate agreements have specifics about how breaches will be handled, and are indemnification agreements in place to ensure that notification and mitigation costs will be covered?				
General Privacy Provisions				
Do employees understand the necessity of disclosing the "minimum amount necessary"?				
Is there personal health information on the outside of patients' charts?				
Are paper charts inaccessible to unauthorized people?				
If sensitive matters are discussed, is there a place to take patients for a more confidential discussion? (Note: never close yourself in a room with just you and a patient. Always bring in another person or leave the door cracked and put someone outside the door to protect you from any false claims or accusations.)				
Do you have authorizations that will allow you to discuss dental and financial matters with those who are financially responsible for others?				
Do employees know never to discuss patients outside the office?				
Are schedules posted in a non-obvious location?				
On sign in sheets, do you ensure that no personal information is asked such as "what is your dental problem today"?				
Is the "Notice of Privacy Policies" posted and available to patients, and did patients sign a form acknowledging receipt?				
Do employees understand that PHI cannot be used for personal reasons?				
Have patients signed authorizations for any photos/x-rays used in your office? (before/after pictures, etc.)				

Action Plan

Item # on Risk Analysis	Actions that need to be taken	Date Completed

Record of Employee Training in OSHA/HIPAA Requirements and other Regulatory Matters

Name of Office: _____

Date/Location of Training: _____

Length of Training: ½ day course

Name of Person Conducting Training: Laney Kay, JD

Summary of Training Session: Annual Bloodborne Pathogen training, satisfying all training elements as required by OSHA; Discussed new infection control guidelines; Q & A on related topics; discussion of evaluating office for potential hazards; discussed epidemiology of bloodborne pathogens, including tuberculosis, AIDS, Hepatitis B and C; discussed Needlestick Requirements, TB Guidelines, discussed engineering controls and evaluated new safety devices; reviewed existing privacy/security standard under HIPAA. Discussed hazard communication standard as required by OSHA, including new pictograms, new labeling and new SDS information. Reviewed fire plan and general hazard communication requirements, including review of chemical hazard requirements and requirement of replacing existing MSDS forms with new SDS ones as they become available.

Reviewed HIPAA regulations, including requirements under Privacy, Security, HI-TECH, and Omnibus Acts.

Name:	**Signature:**