2020 OSHA, HIPAA, Bloodborne Pathogen training

Integral Training, LLC

HIPAA
Knock, Knock…

1996 Health Insurance Portability and Accountability Act (**HIPAA**) was created for healthcare.

The primary goal of the law:

to make it easier for people to keep health insurance,

protect the confidentiality security of healthcare information

help the healthcare industry control administrative costs.

The best known regulation is the HIPAA Privacy Rule-April 2003.

In addition there is a HIPAA Security Rule-April 2005 the HITECH Breach Notification Rule-February 2010

OMNIBUS Rule-January 2013

HITECH SECURITY

The Privacy Rule

THE SECURITY RULE

HIPAA ENFORCEMENT RULE

THE BREACH NOTIFICATION RULE

OMNIBUS=Final Rule 2013

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights announces a final rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- Extends the requirements of the privacy and security rules to covered dental practices' business associates and their contractors
- Establishes limitations on the use of PHI for marketing and fund-raising purposes
- Prohibits the sale of a patient's PHI
- Expands patients' rights to request and receive electronic copies of their PHI
- Broadens patients' ability to restrict disclosure of their personal health information to health insurance plans

Breach Prevention

BEST WAY TO KEEP PERSONAL HEALTH INFORMATION SAFE

Step 1: Develop a Written Policy
Step 2: Assign a Contact Person
Step 3: Team Training
Step 4: Business Associate Safeguards
Step 5: Posting of HIPAA Privacy Policy
Step 6: Patient Acknowledgement, or refusal, of Privacy Policy
Step 7: Self Audits
Step 8: Authorization and Record Keeping Logs for Use of PHI for Other Than Third Party Organization

HIPAA Access

You DO need to worry about verbal communications involving Protected Health Information ("PHI") even if verbal discussions are not governed by the HIPAA Regulations.

You're free to access and share PHI only if it is part of your job and can only be shared with individuals who need the information

All employees are responsible for complying with the HIPAA policies implemented in entities in which they work.

Patients may authorize disclosure of health information to specify family members or friends in writing on the designated Form.

In most cases, disclosures of PHI under the special circumstances categories must be documented.

HIPAA safety and security

- You can look at patient information as long as it's part of your job.
- Accessing patient information electronically can be tracked back to your User ID and computer.
- Unsecured Protected Health Information can include information in any form or medium, including electronic, paper or verbal.
- A Breach is considered the first day that it is known.

(or reasonably should have been known) by the Covered Entity or Business Associate

HIPAA Penalties

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Top Ten 2019 breaches…so far

Rank	Name of Covered Entity	Covered Entity Type	Individuals Affected	Type of Breach
1	AMERICAN MEDICAL COLLECTION DATA BREACH (Quest, LabCorp, etc))	Collection Agency	25 million	**Hacking** (8 months before discovered)
2	DOMINION NATIONAL	Health Plan Provider	2.96 million	**Unauthorized Access** (alert, breach dated 9 years back)
3	INMEDIATA HEALTH GROUP	Healthcare Group	1.5 million	**Compromised Database** (search engine malfunction, w/ wrong patients getting letters)
4	UNIVERSITY OF WASHINTON MEDICINE	Healthcare Group	973,024	**Compromised Database** (misconfigured server)
5	WOLVERINE SOLUTIONS GROUP	Health Related Client Services	600,000	**Ransomware**

Top Ten 2019 breaches…so far

Rank	Name of Covered Entity	Covered Entity Type	Individuals Affected	Type of Breach
6	OREGON DEPARTMENT OF HUMAN SERVICES	HHS	645,000	**Phishing** (9 employees responded to malicious emails)
7	COLUMBIA SURGICAL SPECIALIST OF SPOKANE	Private Practice	400,000	**Hacking** (with ransomware, ransom not paid)
8	UCONN HEALTH	Healthcare Group	326,629	**Phishing** (emails again)
9	NAVICENT HEALTH	Group Practice	278,016	**Unauthorized Access** (third party access)
10	ZOLL SERVICES	Medical Device Vendor	277,319	**Database Exposed** (server migration error)

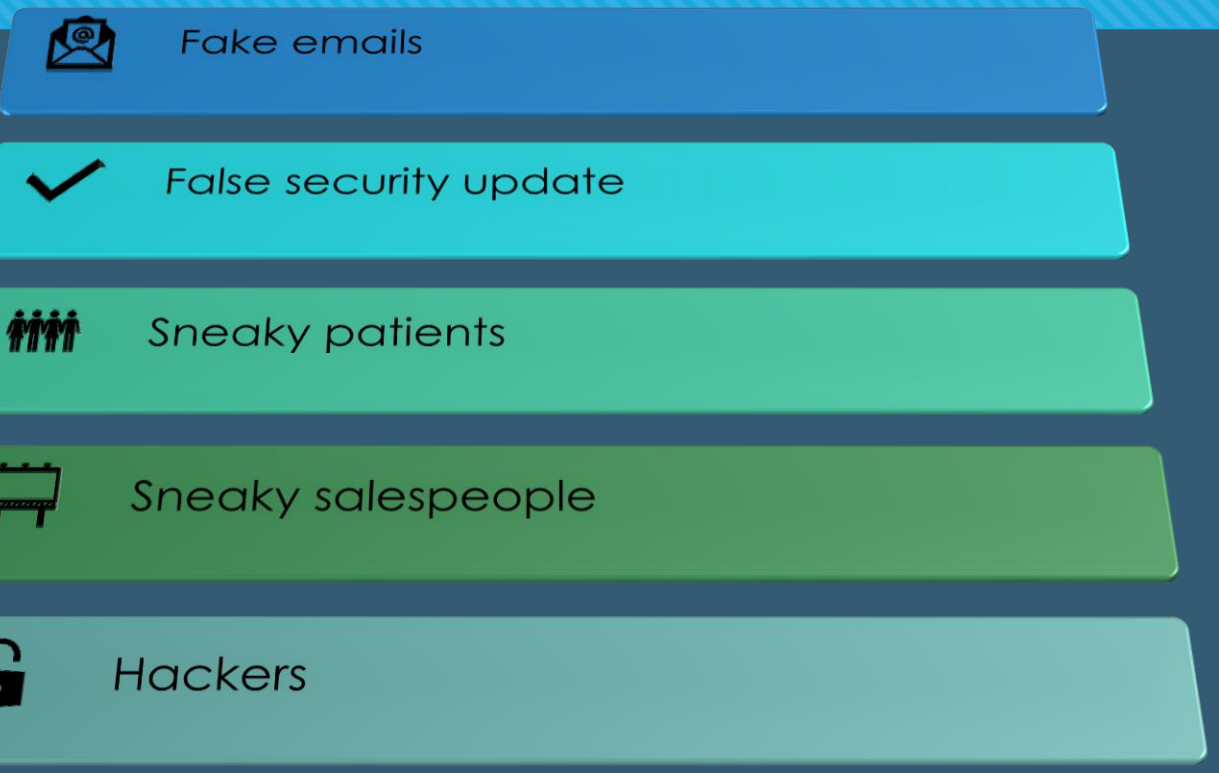
Who has breaches

The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency:

- **Private Practices***
- General Hospitals
- Outpatient Facilities
- Pharmacies

Most common breach?

- Impermissible uses and disclosures
- Lack of safeguards
- Lack of patient access to their protected health information
- Lack of administrative safeguards of electronic PHI
- Use or disclosure of more than the minimum necessary PHI



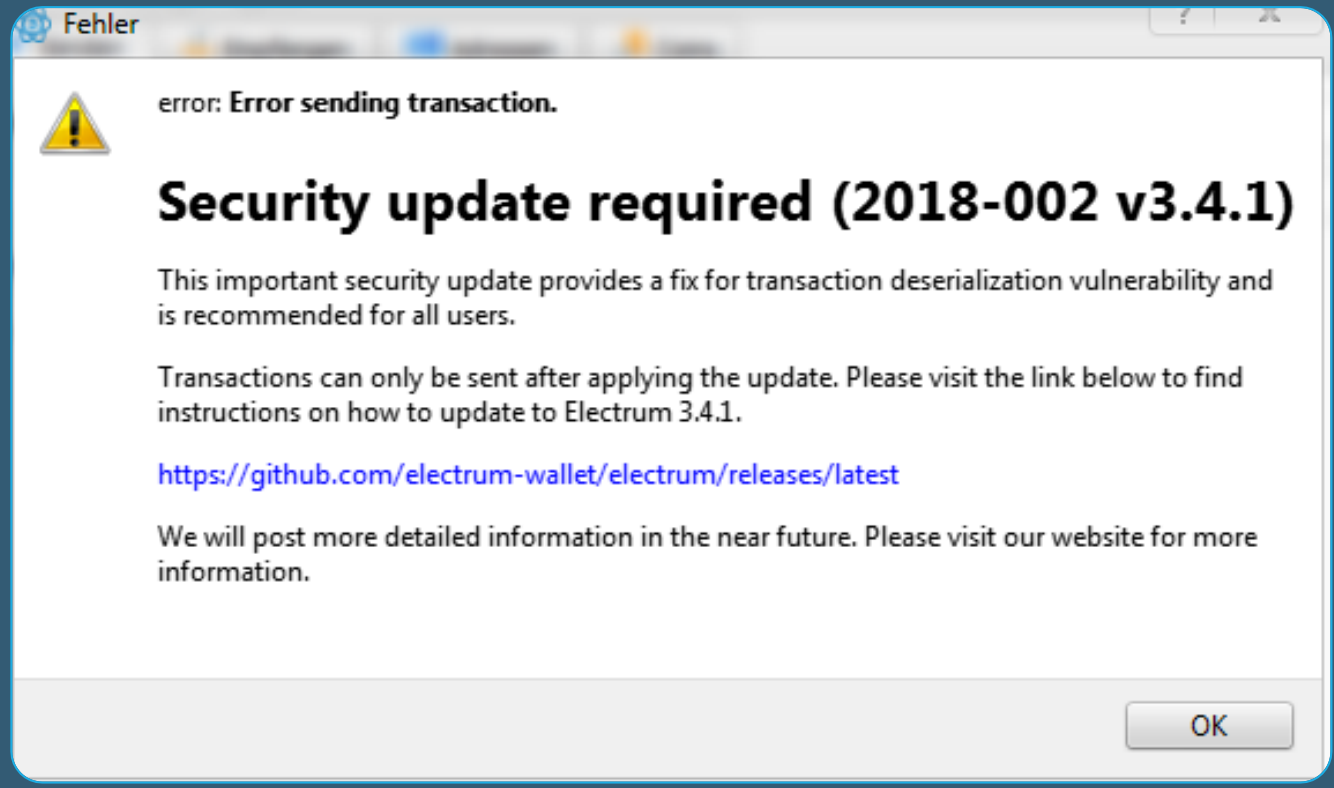
How does this happen?

FAKE EMAILS

- Do not click link in an email unless you know where it came from .
- Always check the sender email if you are unsure.
- Call your IT company immediately if you suspect you clicked something.

FAKE SECURITY UPDATE

- Do not click anything that looks like a security update.
- Always check with your IT people, they will let you know if there is an update and they will install it.
- Just click the “x” to close it, or let it disappear on its own.
- If you are locked out of anything because of a potential update, call your IT company immediately.



SNEAKY PATIENTS

- Lock your computer screen each and every time you leave the patient room.
- Some people will take a picture of the screen, or look to see what information they can find

SNEAKY SALESPEOPLE

- Be careful if a new rep shows up, and offers you promotional thumb drives.
- The newest trend is free, new or promotional thumb drives containing a virus.
- When you go to use them all your information is taken encrypted.

HACKERS

- Having robust security policies, procedures and safeguards in place.
- Use caution, common sense and utilize your IT vendor.
- Annual training helps be aware of the latest trends.
- IT vendor, VPN, Could backup, nothing stored on desktops, shared drive

Recap

- Prevention and training are key.
- Have an offsite back up.
- Not clicking anything you are unsure of.
- Do no give out any information to any unauthorized people.
- Do not use flash drives to store PHI
- Do not use someone else's password or access.
- Report a breach the minute you identify it.
- Do not send any patient information via mobile phone, text or photo.

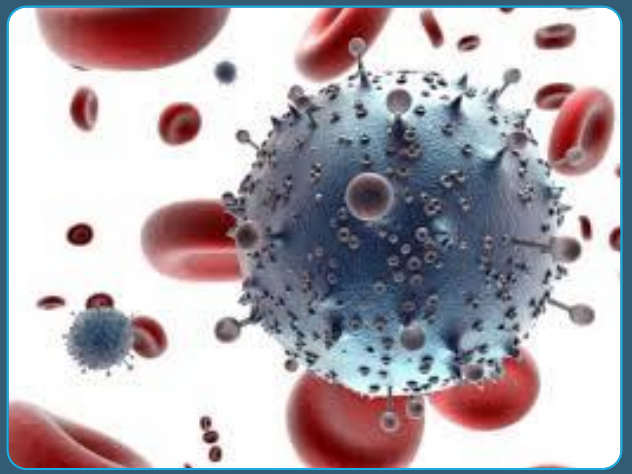
Palate Cleanser

Bloodborne Pathogens:

- Bloodborne Pathogens are pathogenic microorganisms that are present in human blood and can cause disease in humans.
- Pathogens include, but are not limited to, HBV, HIV & Influenza.

Employee Hepatitis-B Vaccination Record:

- All vaccinations up to date?
- Hep B
- Flu? not required, if you give it keep an authorization on file
- Tetanus? Also not required, if you give it keep an authorization on file



Contaminated/Decontaminated:

- Contaminated means the presence or the reasonably anticipated presence of blood or other potentially infectious materials on an item or surface.
- Decontamination means the use of physical or chemical means to remove or destroy bloodborne pathogens on a surface or item to the point where they are no longer capable of transmitting infectious particles, and the surface or item is rendered safe for handling, use or disposal.
- Several methods of decontaminating are chemical disinfecting, dry heat/steam sterilization, and proper disposal of disposable barriers.

Cross-Contamination:

- Cross-contamination is the passage of pathogens indirectly from one patient to another due to use of improper sterilization/disinfecting procedures, unclean instruments, or recycling of products.
- Work surfaces that become contaminated with blood or other bodily fluids can expose someone to bloodborne diseases.
- Reduce Cross-Contamination by:
  - Disinfecting surfaces that may have been in contact with blood or body fluids.
  - Changing gloves after contact with the patient.
  - Refraining from touching personal items, such as pens, cell phones and hair when wearing gloves

Dried blood on a counter top… why be worried about?

- Certain bloodborne viruses can live for days outside the body and still cause infection.
- Hep-B can live in dried blood for up to a week. Hep-C virus can survive for up to 4 days.

Applying Universal Precautions

UNIVERSAL PRECAUTIONS IS AN APPROACH TO INFECTION CONTROL.

ALL HUMAN BLOOD AND BODY FLUIDS NEED TO BE TREATED AS IF IT IS INFECTED WITH HIV, HBV, AND/OR OTHER BLOODBORNE PATHOGENS.

ALWAYS USE APPROPRIATE PPE INCLUDING: GLOVES, GOWNS, MASKS, AND EYE PROTECTION

New Covid Precautions

Well Patients

DENTAL PROCEDURES NOT INVOLVING AEROSOL-GENERATING PROCEDURES

WORK CLOTHING, SUCH AS SCRUBS, LAB COAT, AND/OR SMOCK, OR A GOWN, GLOVES

EYE PROTECTION (E.G., GOGGLES, FACE SHIELD)

FACE MASK (E.G., SURGICAL MASK)

DENTAL PROCEDURES THAT MAY OR ARE KNOWN TO GENERATE AEROSOLS

GLOVES, GOWN

EYE PROTECTION (E.G., GOGGLES, FACE SHIELD)

NIOSH-CERTIFIED, DISPOSABLE N95 FILTERING FACEPIECE RESPIRATOR OR BETTER*

Patients with suspected or confirmed COVID-19

DENTAL PROCEDURES NOT INVOLVING AEROSOL-GENERATING PROCEDURES

GLOVES, GOWN

EYE PROTECTION (E.G., GOGGLES, FACE SHIELD)

NIOSH-CERTIFIED, DISPOSABLE N95 FILTERING FACEPIECE RESPIRATOR OR BETTER*

DENTAL PROCEDURES THAT MAY OR ARE KNOWN TO GENERATE AEROSOLS

GLOVES, GOWN

EYE PROTECTION (E.G., GOGGLES, FACE SHIELD) NIOSH-CERTIFIED, DISPOCABLE N95 FILTERING FACEPIECE RECPIRATOR OR BETTER*

PREVENTION:

- Receive Hepatitis B vaccine:
  Hepatitis B can survive on a dried surface up to one week.

- Never recap needles using two hands; instead use:
  The Scoop method
  Needle recapper

- Dispose of sharps in designated sharps containers.

- PPE:
  Wear gloves
  Eye protection for operator, patient and anyone present in operatory
  Face mask properly worn over nose
  Gown

- Disinfectant operatory/patient care area.

Safe Work Practices:

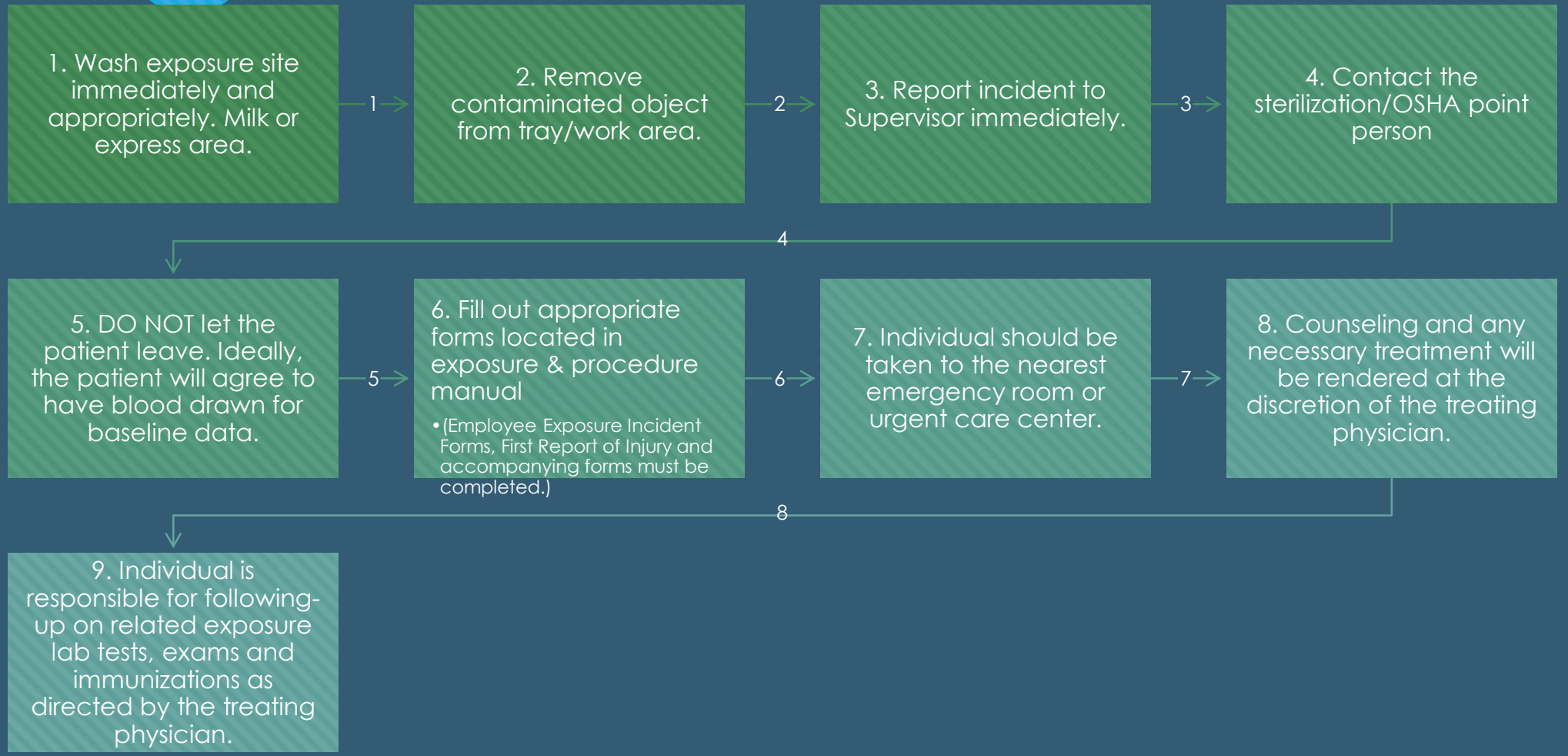
- When performing emergency dental care, dental care workers should follow all appropriate precautions for dentistry and healthcare workers, as well as ensuring appropriate bloodborne pathogen standards are followed when encountering saliva and blood.
- Minimize using, or do not use without appropriate precautions, dental handpieces and air-water syringes. The use of ultrasonic scalers is not recommended during this time. Prioritize minimally invasive/atraumatic restorative techniques (hand instruments only).
- If aerosol-generating procedures are necessary for emergency dental care, use high evacuation suction and dental dams to minimize droplet spatter and aerosols.
- Perform as many tasks as possible in areas away from patients and individuals accompanying patients (e.g., do not remain in a patient care area to perform charting, sterilization, or other tasks).
- Workers should avoid touching their faces, including their eyes, noses, and mouths, particularly until after they have thoroughly washed their hands after completing work and/or removing PPE.
- Train and retrain workers on how to follow established protocols.

Exposure Incident:

- Exposure Incident means that there has been contact with blood or other potentially infectious material.

- Routes of entry can be via an eye, mouth, non-intact skin, or other mucous membrane, or by means of piercing the skin barrier thorough such events as needlesticks, human bites, cuts and abrasions.

EMPLOYEE Exposures: (Exposure Policy & Procedures Manual)



Sharps Containers:

- What goes in the sharps containers?

  * Hypodermic needles
  * Syringes with needles attached
  * Scalpels
  * Blood vials
  * Broken glassware
  * Dental wires
  * IV tubing, needleless connectors, barrel syringes without a needle
  * IV bags contaminated with visible blood

Red Bags:

- What goes into the red bags?

* Biomedical waste; including blood, tissues from humans or animals, and biological waste such as virus or bacteria cultures, bodily fluids or excrement.

* Visibly bloody gloves, plastic tubing, or personal protective equipment (PPE).

* Gauze, bandages or other items saturated with blood.

*remember this is weighed, so no regular trash

SPILLS:

- Chemical spill kits located in Sterilization Department.
- Body fluids need to be cleaned with water and 10% bleach.

TO CLEAN SPILL YOU WILL NEED:

- Goggles
- Utility Gloves
- Mask
- Paper Towels
- Red Bag

STERILIZATION MONITORING:

- Record:
  - Cycle time
  - Temperature
  - Pressure
- Date all packaging.
- For multiple sterilizers- label the outside of packaging with the sterilizer name/number used.
- Spore test:
  - Must be done every 40hr and logged for reference.

Labeling Containers:

- OSHA requires that biohazard markings be affixed to containers of regulated waste, refrigerators and freezers containing blood, and other containers used to store, transport or ship blood or other potentially infectious materials.

- The background must be fluorescent orange or orange-red or predominantly so, with symbols and lettering in a contrasting color.

Safety Data Sheets:

- SDS: Safety Data Sheets (no more MSDS)
- Must be kept on all Hazardous chemicals.
- If contents from one container are transferred to another container, a new label must be prepared using the SDS information.
- Labeling should include name of product along with appropriate warnings.

FOOD and/or DRINKS:

- Food and/or Drinks are NOT allowed to be kept in:
  - **Refrigerators**
  - **Freezers**
  - **Shelves**
  - **Cabinets**

Where blood or other potentially infectious materials may be present.

- HBV can survive dried on an environmental surface for up to one week.
- Standard/Universal precautions means treating all blood and any body fluids as potentially infectious.
- Never hand-recap needles.
- Do NOT store your food and drink close to you when working with blood so you don't have to leave the room.
- If you are exposed and know where the blood came from, You are obligated to report it.
- People carrying bloodborne pathogens can look and feel healthy.
- Receive the hepatitis B vaccine before a sharps injury occurs.
- Every used sharp should be treated as though it could transmit a bloodborne disease. Uncontaminated sharps are disposed in sharps container.
- Lock and label all sharps containers when ¾ filled.

recap

- Have bloodborne pathogen training and active plan
- Train and screen all employees on office policies
- Report any and all OSHA/HIPAA violations to the point person the moment they are identified. The violation policy should then be followed.
- Ensure business associate agreements are in place and adhered to.
- Monitor all policy, procedure and protocol are followed by spot checks and chart audits.
- Violations can happen to anyone at any time. Preparation is key.

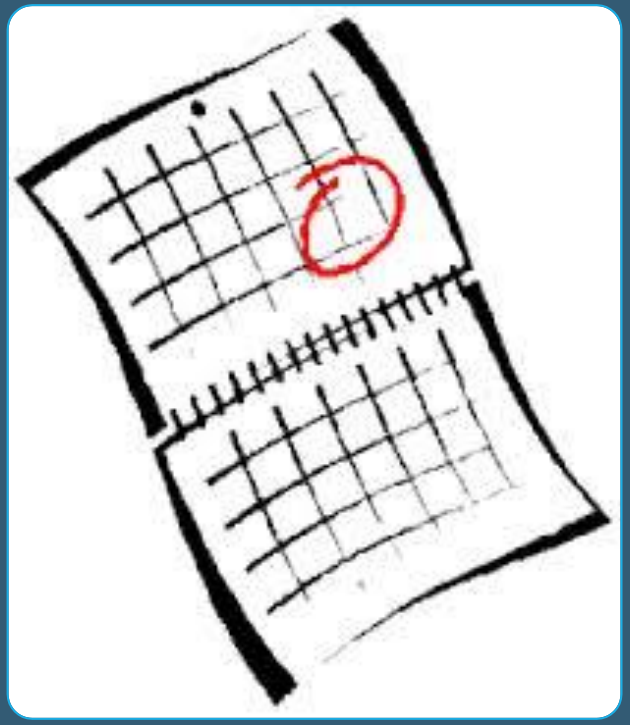
Any Questions?

Sources of Information:

- www.cdc.gov center for disease control and prevention
- http://www.ada.org American Dental Association
- www.cdc.gov/niosh/npg/ national institute of occupational safety and health
- www.OSHA.gov occupational safety & health administration
- http://www.hhs.gov U.S. Department of Health & Human Services
- https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/ProvCmpl_Products.pdf
- Office Post Exposure Policy & Procedure.

OSHA & HIPAA Certificates:

- To be completed by all Employees and associates
- Once you have completed this module, you will need to keep sign in sheet in your records.
- This course is mandatory for and must be renewed annually.




Thank you!