Test Your Bloodborne

2001940

Pathogens Knowledge

TEST

Directions: Complete each of the following statements using the word bank below. Write your answers on the lines.

Word Bank

Sexual contact Bloodborne pathogens Damaged Red Medical examination
Blood Bodily fluids Blood test Hep B Universal Precautions
Exposure control plan Decontamination and cleaning schedule

1. _____ _____ are microorganisms carried by the blood, such as the hepatitis virus (HBV and HCV) and the human immunodeficiency virus (HIV).
2. Your employer has established a written _____ _____ _____ that follows regulations set up by the federal Occupational Safety and Health Administration.
3. To protect yourself against HIV and Hepatitis, avoid direct exposure to _____ and _____ _____ the prime transmitters of HIV and hepatitis.
4. HIV and hepatitis can be transmitted through _____ _____, shared drug needles, needle stick injuries, and direct contact between broken or chafed skin and infected body fluids.
5. _____ _____ means you treat all blood and other potentially infectious body fluids as if they are infected.
6. Before you put on protective clothing, make sure it is in good condition. Do not wear anything that is _____.
7. Your employer's written _____ _____ _____ _____ helps keep your workplace free of infection.
8. To make sure you know what you are handling, OSHA requires containers of potentially infectious materials to be _____, or labeled clearly in orange or orange-red with the biohazard symbol or both.
9. If you are directly exposed to bloodborne pathogens, your employer will offer you a confidential _____ _____ and _____ _____.
10. There is a vaccine that helps protect against_____, and OSHA requires employers to provide it free to employees at risk of exposure.

Name: _____ Date: _____ Grade: _____

Name_____ Date_____

Cultural Diversity in Health Care Information Sheet

Culture is the values, beliefs, standards, language, thinking patterns, behavioral norms, communication styles, etc. shared by a group of people. It guides decisions and actions of a group through time. We have an obligation to be respectful and sensitive to another's belief system. Healthcare workers must be culturally competent and comfortable with those they serve. Healthcare workers should understand how their own personal biases and values influence communication with patients, families, and co-workers. All agency staff will be trained to identify patients with any language barriers which may prevent effective communication of the rights and responsibilities.

Cultural Sensitivity is the ability to be open to learning about and accepting of different cultural groups.

Multiculturalism is the recognition and acknowledgement that society is pluralistic. In addition to the dominant culture, there exists many other cultures based around ethnicity, sexual orientation, geography, religion, gender, and class.

Cultural competence is the understanding of diverse attitudes, beliefs, behaviors, practices, and communication patterns attributable to a variety of factors (such as race, ethnicity, religion, historical and social context, physical or mental ability, age, gender, sexual orientation, or generational and acculturation status). A health care provider is culturally competent when he/she is able to deliver culturally appropriate and specifically tailored care to patients with diverse values, beliefs, and behaviors.

Ask yourself the following questions when you are acquiring cultural competence: Who are my patients, families, and coworkers? How can I learn about them? What are my beliefs about this group? In order to acquire knowledge of the cultural values, beliefs and practices of your patients you must: ask questions, listen, account for language issues, and be aware of communication styles to include language barriers and literacy level. You must also consider body language through eye contact, touching, personal space, privacy/modesty, gender, wealth or social status, presence of a disability, and sexual orientation.

Acquiring cultural competence includes: Being sensitive to personal health beliefs and practices to include: Special foods, drinks, objects and clothes, avoidance of certain foods, people or places, customary rituals or people uses to treat the illness, compliance with taking medicine even if he/she doesn't feel sick, knowledge of who in the family is making decisions about health care and are their illnesses treated at home or by a community member.

Ways to facilitate communication across cultural boundaries include: recognize differences, build your self-awareness, describe and identify, then interpret, don't assume your interpretation is correct, verbalize your own non-verbal signs, share your experience honesty, acknowledge any discomfort, hesitation, or concern, practice politically correct communication, give your time and attention when communicating, and do not evaluate or judge.

It is because we are different that each of us is special!

Name _____ Date_____

Cultural Diversity in Health Care Quiz

1. The values, beliefs, standards, language, thinking patterns, behavioral norms, communication styles, etc. shared by a group of people is:
   Culture Tradition Ethics

2. The ability to be open to learning about and accepting of different cultural groups is:
   Awareness Cultural Sensitivity Obligation

3. A health care provider is culturally competent when he/she is able to deliver culturally appropriate and specifically tailored care to patients with diverse values, beliefs, and behaviors.
   True False

4. Acquiring cultural competence includes: Being sensitive to personal health beliefs and practices to include: special foods, drinks objects and clothes, avoidance of certain foods, people or places.
   True False

5. Ways to facilitate communication across cultural borders includes all of the following: recognize differences, build your self-awareness, describe and identify, then interpret, and don't assume your interpretation is correct. You should contact your clinical supervisor in order to obtain access to the CTS language link translation line.
   True False

Continuum
PEDIATRIC NURSING

BLOODBORNE PATHOGENS AT A GLANCE

	Hepatitis B Virus (HBV)	Hepatitis C Virus (HBV)	Hepatitis D Virus (HDV)	Human Immunodeficiency Virus (HIV)	Syphilis
Epidemiology	300, 00 new U.S. cases and 15,000-20,000 new carrier annually. Most common Bloodborne pathogen with risk to healthcare workers (HCW) (6-30% risk for infection for needle stick injury with infected source blood).	170,000 new U.S. cases annually. 4-8% of cases are HCW who acquired disease occupationally	Causes infection only together with HBV.	Worldwide 18 million adults and 1.5 million children are infected (90% of cases are in developing countries). New U.S. cases 40,000-80,000 annually. Risk of HCW infection from needle stick injury with infected source blood is estimated to be 0.32%	Widespread. Approximately 30% of exposures result in infection.
Modes of Transmission	Blood-to-blood contact; sexual contact; perinatal transmission; contact with contaminated objects (40% unknown; thought to be person-to-person contact with mucous membrane or non-intact skin)	Blood-to-blood contact; sexual contact; contact with contaminated objects	Believed to be similar to HBV	Sexual contact; prenatal transmission; blood-to-blood contact; contact with contaminated objects (e.g., needles).	Sexual contact; contact with infectious exudates, body fluids and secretions; congenital transmission; blood-to-blood contact; contacts with contaminated objects.
Infectious Agent	Hepatitis B Virus	Hepatitis C Virus	Hepatitis D Virus	Human Immunodeficiency Virus	Treponema pallid, a spirochete
Period of Communicability	Begins before symptoms appear and persist throughout course of disease and during chronic carrier state.	Begins before symptoms appear and persist throughout course of disease and during chronic carrier state.	Blood is potentially infectious during all phases of infection	Presumed to being early in infection and extend throughout life	Variable and indefinite. Adequate penicillin therapy ends inactivity in 24-48 hrs
Incubation Period	30-180 days	14-180 days	Not firmly established in humans	Variable; time from infection to development of AIDS ranges from 2 mo. To 10 yrs. Or longer	10 days-3 months

Signs and Symptoms	Anorexia, abdominal discomfort, nausea and vomiting. Prodromal rash and arthritis (5-10%). Often progress to jaundice. Fever absent or mild.	Anorexia, abdominal discomfort, nausea and vomiting. Progress to jaundice less often than hepatitis B	Similar to HBV	Self-limited mononucleosis-like illness within several weeks to several months after infection. Onset of clinical illness characterized by lymphadenopathy, anorexia, chronic diarrhea, weight loss, fever and fatigue. Opportunistic infection several cancers define AIDS	An acute and chronic disease characterized by a primary skin lesion (chancre), secondary eruptions of skin and mucous membranes, long latency periods, and late lesions of skin, bone internal organs, nervous system and cardiovascular system.
Post exposure Management	If unvaccinated, HBV vaccine and immune globulin. If vaccinated, recommendations depend on response to vaccine	Immune globulin of unproven value	Prevention of HBV	Consider antiretroviral therapy based on nature of exposure	Penicillin treatment or alternatively, treatment with doxycyline or tetracycline
Complications and Prognosis	Usually mild disease with full recovery; development of chronic carrier state may occur fatal in about 0.1% cases. Risk factor for liver cancer	High rate of chronic carriers (50-80%); generally a full recovery in others	Infection with HBV and HDV increases risk of serious illness or death	No recovered cases conclusively documented; degree of immunity unknown.	Treatable with antibiotics. Untreated diseases may result in serious disability or death.
Prevention	HBV vaccine for all infants, HCW, and other risk. Avoid exposure by screening donated blood; condom use; work practice and engineering controls to minimize risk to HCW; personal protective equipment for HCW	No vaccine available. Avoid exposure (see measures outline for HBV); screening donated blood	Same as HBV	No vaccine available. Avoid exposure (see measures outline for HBV); screening donated blood	STD control measures. Avoid exposure

Print name Signature Date

Fraud, Waste and Abuse Quiz

Name_____ Date_____ Grade_____

Please choose either True or False.

1. ☐ True ☐ False - CMS is the part of the federal government that oversees the Medicare and Medicaid programs.

2. ☐ True ☐ False - Medicare/ Medicaid will not pay a provider who has been excluded by the OIG from participation in a federal health care program.

3. ☐ True ☐ False - Fraud is: An intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some authorized benefit to himself or some other person.

4. ☐ True ☐ False - If I identify, or I am made aware of potential misconduct or a suspected fraud, waste or abuse situation, I should keep this information to myself and not tell anyone else.

5. ☐ True ☐ False - The effort to prevent and detect fraud is a cooperative effort involving CMS, Medicare/ Medicaid providers, and health plans.

6. ☐ True ☐ False - The FBI has the authority to exclude (sanction) providers or suppliers who have been convicted of health care related offenses.

7. ☐ True ☐ False - Whistleblower protection provides you with the right to report suspected fraud, waste or abuse but only with a chance of retaliation.

8. ☐ True ☐ False - Waste is a practice that results in unnecessary costs.

9. ☐ True ☐ False - The following are all examples of fraud, waste and abuse: Medical identity theft, billing for unnecessary services or items, billing for services or items not rendered, up coding, unbundling, billing for non-covered services or items, kickbacks and beneficiary fraud.

10. ☐ True ☐ False - Providers play an important role in preventing fraud, waste and abuse.

Name_____ Date_____

Fraud, Waste and Abuse Training Information

CMS (Center for Medicare and Medicaid Services) is part of the federal government that oversees the Medicare and Medicaid programs.

Abuse is defined in the CMS rules as: Provider practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost to the Medicare/Medicaid program, or reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. Abuse includes: Excessive or improper use of resource, intentional destruction, diversion, manipulation, misapplication, or misuse of resources, and extravagant or excessive use as to abuse one's position or authority. It also includes beneficiary practices that result in unnecessary cost to the Medicare/Medicaid programs. A provider can abuse the Medicare/Medicaid program even if there is no intent to deceive.

Fraud is different and involves intent. Waste is a practice that results in unnecessary costs.

Providers, beneficiaries, corporate officials and others can commit health care fraud. The rules governing Medicaid define fraud as: An intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some authorized benefit to himself or some other person. It includes any act that constitutes fraud under applicable Federal or State law.

Health care fraud is defined in Title 18, US Code 1347 as knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program or to obtain (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the custody or control of, any health care benefit program.

The Federal False Claims Act (FFCA) protects the Federal Government from being overcharged or sold substandard goods or services. The FFCA imposes civil liability on any person who knowingly submits, or causes the submission of a false or fraudulent claim to the Federal Government. The terms “knowing” and “knowingly” mean a person has actual knowledge of the information or acts in deliberate ignorance or reckless disregard of the truth or falsity of the information related to the claim. No proof or specific intent to defraud is required to violate the civil FFCA. There is also a criminal FFCA statue by which individuals or entities that submit false claims may face fines, imprisonment, or both.

Fraud, waste and abuse in the Medicaid program may occur in many different ways including: Medical identity theft, billing for unnecessary services or items, billing for services or items not rendered, up coding, unbundling, billing for non-covered services or items, kickbacks and beneficiary fraud.

If an entity is convicted of Medicare/ Medicaid fraud the OIG (Office of Inspector General) has the authority to exclude individuals and entities from federally funded health care programs.

Everyone has the right and responsibility to report possible fraud, waste and abuse. Whistleblower protection provides you with the right to report suspected fraud, waste or abuse without retaliation. Please report any concerns to the Chief Compliance Officer @ 703-506-0123. Providers play an important role in preserving the solvency of the Medicaid program, protecting beneficiaries from harm, and preventing fraud, waste and abuse.

Hand Hygiene Quiz

Name:_____ Date:_____

1. When hands are visibly soiled or dirty, you should perform hand hygiene using:

   - ☐ Soap and water
   - ☐ Alcohol based hand rub
   - ☐ Water only

2. If your hands are not visibly contaminated, you may use an alcohol based hand rub for performing hand hygiene.

   - ☐ True
   - ☐ False

3. Infectious agents such as bacteria, viruses, fungi, and parasites can be transferred to your hands by touching a contaminated object such as a doorknob.

   - ☐ True
   - ☐ False

4. Which of the following is correct regarding glove usage?

   - ☐ You don't need to wash your hands after you remove your gloves
   - ☐ It is acceptable to use the same pair of gloves for more than one patient
   - ☐ You should wear gloves when you suspect you will contact body fluids
   - ☐ Gloves don't help to protect against infection

5. You should perform hand hygiene after you:

   - ☐ Change a diaper
   - ☐ Use the restroom
   - ☐ Clean spilled formula off of the floor
   - ☐ All of the above

6. Why should artificial nails not be worn by people providing patient care?

- [ ] They are hard to clean
- [ ] They can tear gloves
- [ ] They can harbor more bacteria than natural, short nails
- [ ] All of the above

7. How are infectious agents most frequently spread from one patient to another?

- [ ] Patients eating in hospital cafeterias
- [ ] Poor environmental maintenance
- [ ] From one patient to another by the contaminated hands of clinical staff
- [ ] Airborne spread from patients sneezing

8. Hand hygiene is the most important way to prevent the spread of germs.

- [ ] True
- [ ] False

9. If you are going to use gloves when caring for your patient, you don't need to perform hand hygiene.

- [ ] True
- [ ] False

10. The primary purpose of hand hygiene is?

- [ ] To keep hands clean
- [ ] To keep nails clean
- [ ] To reduce the amount of microorganisms on hands
- [ ] To make hands smell nice

The CDC Guideline for Hand Hygiene in Healthcare Settings

Indications for Hand Washing and Hand Antisepsis:

A. When hands are visibly dirty or contaminated with proteinaceous material or are visibly soiled with blood or other body fluids, wash hands with either a non-antimicrobial soap and water or an antimicrobial soap and water
B. If hands are not visibly soiled, use an alcohol-based hand rub for routinely decontaminating hands in all other clinical situations described in items C-J. Alternatively, wash hands with an antimicrobial soap and water in all clinical situations described in items C-J
C. Decontaminate hands before having direct contact with patients
D. Decontaminate hands before donning sterile gloves when inserting a central intravascular catheter
E. Decontaminate hands before inserting indwelling urinary catheters, peripheral vascular catheters, or other invasive devices that do not require a surgical procedure
F. Decontaminate hands after contact with a patient's intact skin (e.g., when taking a pulse or blood pressure, and lifting a patient)
G. Decontaminate hands after contact with body fluids or excretions, mucous membranes, nonintact skin and wound dressings if hands are not visibly soiled
H. Decontaminate hands if moving from a contaminated-body site to a clean-body site during patient care
I. Decontaminate hands after contact with inanimate objects (including medical equipment) in the immediate vicinity of the patient
J. Decontaminate hands after removing gloves
K. Before eating and after using a restroom, wash hands with a non-antimicrobial soap and water or with an antimicrobial soap and water
L. Antimicrobial-impregnated wipes (i.e., towelettes) may be considered as an alternative to washing hands with non-antimicrobial soap and water. Because they are not as effective as alcohol-based hand rubs or washing hands with an antimicrobial soap and water for reducing bacterial counts on the hands of HCWs, they are not a substitute for using an alcohol-based hand rub or antimicrobial soap
M. Wash hands with non-antimicrobial soap and water or with antimicrobial soap and water if exposure to Bacillus anthracis is suspected or proven. They physical action of washing and rinsing hands under such circumstances is recommended because alcohols, chlorhexidine, iodophors, and other antiseptic agents have poor activity against spores
N. No recommendation can be made regarding the routine use of nonalcohol-based hand rubs for hand hygiene in health-care settings. Unresolved issue.

Hand Washing Procedure with Liquid or Foam Soap:

1. Wet hands first with water.
2. Apply enough soap sufficient to cover all surfaces of hands and wrists.
3. Rub hands for a minimum of 15 seconds vigorously to generate friction.
4. Lather every surface well; especially around the nails.
5. Rinse well with running water.
6. Dry thoroughly with paper towel.
7. Use paper towel to turn off faucet.
8. Avoid using hot water as repeated exposure to hot water may increase risk of dermatitis.

*Liquid, bar, leaflet or powdered forms of plain soap are acceptable when washing hands with a nonantimicrobial soap and water. When bar soap is used, soap racks that facilitate drainage and small bars of soap should be used.

**In the absence of water, use alternative agents like detergent containing towelettes (for removal of light soil) and alcohol based hand rubs (for reduction of microbial flora). Do not use hand rubs if hands are soiled.

Decontamination Procedure with Alcohol-Based Hand Rubs:

1. Apply product to palm of one hand and rub hands together, covering all surfaces of hands and fingers, until hands are dry.
2. Follow the manufacturer's recommendations regarding the volume of product to use.

Other Aspects of Hand Hygiene:

A. Do not wear artificial fingernails or extenders when having direct contact with patients at high risk (e.g., those in intensive-care units or operating rooms).
B. Keep natural nails tips less than 1/4 –inch long.
C. Wear gloves when contact with blood or other potentially infectious materials, mucous membranes and nonintact skin could occur.
D. Remove gloves after caring for a patient. Do not wear the same pair of gloves for the care of more than one patient, and do not wash gloves between uses with different patients.
E. Change gloves during patient care if moving from a contaminated body site to a clean body site.
F. No recommendation can be made regarding wearing rings in healthcare setting. Unresolved issue.

Definition of Terms:

Alcohol-Based Hand Rub: An alcohol containing preparation designed for application to the hands for reducing the number of viable microorganism on the hands. In the United States, such preparations usually contain 60%-95% ethanol or isopropanol.
Antimicrobial Soap: Soap (i.e., detergent) containing an antiseptic agent.
Antiseptic agent: Antimicrobial substances that are applied to the skin to reduce the number of microbial flora. Examples include alcohols, chlorhexidine, chlorine, hexachlorophene, iodine, chloroxylenol (PCMX), quatemary ammonium compounds, and triclosan.
Antiseptic Hand Wash: Washing hands with water and soap or other detergents containing an antiseptic agent.
Antiseptic Hand Rub: Applying an antiseptic hand-rub product to all surfaces of the hands to reduce the number of microorganism present.
Cumulative Effect: A progressive decrease in the numbers of microorganism recovered after repeated applications of a test material.
Decontaminate Hands: To reduce bacterial counts on hands by performing antiseptic hand rub or antiseptic hand wash.
Detergent: Detergents (i.e., surfactants) are compounds that possess a cleaning action. They are composed of both hydrophilic and lipaphilic parts and can be divided into four groups;: anionic, cationic , amphoteric, and nonionic detergents. Although products used for hand washing or antiseptic hand wash in health-care settings represent various types of detergents, the term "soap" is used to refer to such detergents in this guideline.
Hand Antisepsis: Refers to either antiseptic hand wash or antiseptic hand rub.
Hand Hygiene: A general term that applies to hand washing, antiseptic hand wash, antiseptic hand rub, or surgical hand antisepsis.
Hand Washing: Washing hands with plain (i.e., non-antimicrobial) soap and water.

Persistent Activity: persistent activity is defined as the prolonged or extended antimicrobial activity that prevents or inhibits the proliferation or survival of microorganism after application of the product. This activity may be demonstrated by sampling a site several minutes or hours after application and demonstrating bacterial antimicrobial effectiveness when compared with a baseline level. This property also has been referred to as "residual activity." Both substantive and nonsubstantive active ingredients can show a persistent effect if they substantially lower the number of bacteria during the wash period.
Plain Soap: Plain soap refers to detergents that do not contain antimicrobial agents or contain low concentrations of antimicrobial agents that are effective solely as preservatives.
Substantivity: Substantivity is an attribute of certain active ingredients that adhere to the stratum corneum (i.e., remain on the skin after rinsing or drying) to provide an inhibitory effect on the growth of bacteria remaining on the skin.
Surgical Hand Antisepsis: Antiseptic hand wash or antiseptic hand rub performed preoperatively by surgical personnel to eliminate transient and reduce resident hand flora. Antiseptic detergent preparations often have persistent antimicrobial activity.
Visibly Soiled Hands: Hands showing visible dirt or visibly contaminated with proteinaceous material, blood, or other body fluids (e.g., fecal material or urine)
Waterless Antiseptic Agent: An antiseptic agent that does not require use of exogenous water. After applying such an agent, the hands are rubbed together until the agent has dried.
Patient Preoperative Skin Preparation: A fast acting, broad-spectrum, and persistent antiseptic-containing preparation that substantially reduces the number of microorganisms on intact skin.
Antiseptic Hand Wash Or HCW Handwash: An antiseptic containing preparation designed for frequent use; it reduces the number of microorganism on intact skin to an initial baseline level after adequate washing, rinsing, and drying; it is broad-spectrum, fast-acting, and if possible, persistent.
Surgical Hand Scrub: An antiseptic containing preparation that substantially reduces the number of microorganisms on intact skin; it is broad-spectrum, fast acting and persistent.

I have read and understand the above information regarding the importance of hand washing.

_____

Print name Signature Date

HIPAA Quiz

Name: _____ Date: _____

1. Which area is not addressed by HIPAA?
   - ☐ Insurance portability
   - ☐ Hospital accreditation
   - ☐ Fraud enforcement
   - ☐ Administrative simplification

2. What does HIPAA define as "covered entities"?
   - ☐ Hospitals only
   - ☐ Hospitals and Payers only
   - ☐ Most providers, clearinghouses and health plans
   - ☐ Providers only

3. What are the 2 types of sanctions under HIPAA?
   - ☐ Security and privacy
   - ☐ Civil and criminal
   - ☐ Accidental and Non-accidental
   - ☐ Serious and non-serious

4. Which organization has been given authority to enforce HIPAA's privacy regulation?
   - ☐ JCAHO
   - ☐ The Office for Civil Rights
   - ☐ The Department of Public Welfare
   - ☐ Local Law enforcement agencies

5. What type of personally identifiable health information is protected by HIPAA's privacy rule?
   - ☐ Oral
   - ☐ Written
   - ☐ Electronic
   - ☐ All of the above

6. When is the patient's authorization required to release information?
   - ☐ In most cases when patient information is going to be shared with anyone for reasons other than treatment, payment or health care operations.
   - ☐ Upon admission to the hospital.
   - ☐ When patient information is used for billing a private insurance.
   - ☐ When information is shared among 2 or more clinicians.

7. Authorization is required to release psychotherapy notes for any reason including treatment.

   ☐ True ☐ False

8. In which case is it acceptable for a hospital to release information without a patient's permission?
   - ☐ When the patient is under 21.
   - ☐ When the person requesting the information is a spouse.
   - ☐ When a nurse suspects child abuse and state laws require providers to report suspected abuse.
   - ☐ When the patient does not live within the state in which they are being treated.

9. Which of the following is considered individually identifiable health information?
   - ☐ Social Security number
   - ☐ Telephone number
   - ☐ Date of Birth
   - ☐ All of the above

10. What should you do if you suspect that someone is violating the organization's privacy policy?
    - ☐ Nothing
    - ☐ Report the individual to the local police department
    - ☐ Take pictures of the offense
    - ☐ Report your suspicions s to the organization's privacy or compliant officer

Continuum Pediatric Nursing Services

HIPAA Training - 2018

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum–Kennedy Act after two of its leading sponsors.

What is the HIPAA Privacy Rule?

"The HIPAA Privacy Rule establishes National standards to protect an individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights
over their health information, including rights to examine and obtain a copy of their health records and to request corrections"

Definition provided by the US Department of Health and Human Services

What is the HIPAA Security Rule?

"The HIPAA Security Rule establishes national standards to protect an individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic Protected Health Information".

Definition provided by the US Department of Health and Human Services

Where the HIPAA Privacy Rule deals with the integrity of PHI in general, the HIPAA Security Rule deals with electronic Protected Health Information (ePHI) and is a response the increasing use of mobile devices in the workplace.

What is the Difference between PHI and ePHI?

While PHI relates to ALL Protected Health Information regardless of its format, *electronic* PHI (ePHI) is defined as all PHI that is stored, transmitted or used electronically.

What is PHI?

PHI stands for Protected Health Information, and is defined as "any information held by a covered entity which concerns health status, the provision of healthcare, or payment for healthcare that can be linked to an individual." But what is this information and who does it apply to?

HIPAA regulations list eighteen different personal identifiers which, when linked together in any combination, are classed as Protected Health Information. These eighteen personal identifiers are:

- Names
- All geographical data smaller than a state
- Dates (other than year) directly related to an individual
- Telephone numbers
- Fax numbers
- E-Mail addresses
- Social Security numbers
- Medical record numbers
- Health insurance plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Device identifiers and serial numbers
- Web URLs
- Internet protocol (IP) addresses
- Biometric identifiers (i.e. retinal scan, fingerprints, Etc.)
- Full face photos and comparable images
- Any unique identifying number, characteristic or code

Enforcement

HIPAA's privacy and security regulations punish individuals and/or organizations that fail to keep patient information confidential.

HIPAA states that "covered entities" must comply with its regulations or they are subject to punishment from the Office of Civil Rights, in the Department of Health and Human Services. These " covered entities" include most providers, health plans and clearing houses.

Anyone who breaks HIPAA's privacy or security rules can be subject civil or criminal sanctions:

Civil penalties can have fines of up to $100 for each violation of a requirement per individual.

How does this affect you? Have you ever read a friend's medical record out of curiosity? Or heard a neighbor was in the hospital and read his chart to see why? These could earn your organization a civil penalty and a fine.

Criminal sanctions can include not only large fines, but also jail time. The penalties can be as high as $250,000 or prison sentences up to 10 years.

Criminal penalties increase as the seriousness of the crime increases. Examples include the selling of a celebrity's medical information to a tabloid, the selling of health information to a pharmaceutical company for personal profit or gaining access to health information under false pretenses.

Communication with or about patients involving patient health information should be private and limited to those who need the information for treatment, payment or health care operations. (Care operations are activities such as medical record reviews, staff performance evaluations, etc.) Only those individuals with an authorized need to know will have access to the protected information. This is frequently referred to as the *Rule of Least Privileged Access.*

Safeguards

WORKSTATIONS

In the eyes of the Department of Health and Human Services, a workstation is any electronic device that can be used to access ePHI. This includes desktop PCs, laptops, tablets, and mobile devices. This definition is not restricted to work issued devices, but **includes any device you use to access ePHI**, even *personal cell phones*.

WORKSTATION SECURITY

All work stations must have appropriate security in place to prevent unauthorized access to ePHI. Typically, this includes:

- Unique Usernames and Passwords
- PIN or Security Codes
- Automatic log out after a predetermined period of inactivity

As above, this **applies to all devices used to access ePHI regardless of who owns the device,** ***Use of unsecured devices by any employee is strictly forbidden.***

STORAGE OF PHI

Any PHI should be safeguarded to protect the patient. This includes:

- Not Leaving Paperwork Unattended
- Not Leaving Paperwork Unsecured
- Paperwork should always be kept under Lock and Key
- If transporting paperwork, it MUST be in a secure container, such as a sealed envelope or locked briefcase.
- If mailing, the envelope must be adequately sealed to ensure unauthorized access has not occurred.
- For electronic PHI this includes:
- ePHI at rest (stored) should be encrypted
- ePHI should be encrypted during transmission
- Continuum policy is that ePHI should never be stored on removable media, local computers (either corporate or private). *Use of a company owned device, is subject to review at any time, for any reason.*

eMail

ePHI should never be emailed except by encrypted communication. Continuum uses such a method when the need to communicate such information with you arises.

SMS/Texting

ePHI should never be communicated this way, unless it is via a closed/secured system approved for such use.

WHAT IS A BREACH?

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and 4. The extent to which the risk to the protected health information has been mitigated.

All suspected breaches are logged and investigated by Continuum to determine if further action is necessary. Any confirmed breach is reported to the HHS Office of Civil rights by Continuum.
The reporting timeline is based on the quantity of patient records exposed, and is covered by the Breach Notification Requirements.

Any breaches must be reported to impacted individuals without unreasonable delay and in no case later than 60 days following the discovery of a breach. If more than 500 individuals are impacted the breach must be reported to the Secretary of HHS without unreasonable delay and in no case later than 60 days following the discovery of a breach. Additionally, all such reported breaches are made public via an HHS website https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

OFFICE FOR CIVIL RIGHTS

SHARING HEALTH INFORMATION WITH FAMILY MEMBERS AND FRIENDS

There is a federal law, called the Health Insurance Portability and Accountability Act of 1996 (HIPAA), that sets rules for health care providers and health plans about who can look at and receive your health information, including those closest to you – your family members and friends. The HIPAA Privacy Rule ensures that you have rights over your health information, including the right to get your information, make sure it's correct, and know who has seen it.

What Happens if You Want to Share Health Information with a Family Member or a Friend?

HIPAA requires most doctors, nurses, hospitals, nursing homes, and other health care providers to protect the privacy of your health information. However, if you don't object, a health care provider or health plan may share relevant information with family members or friends involved in your health care or payment for your health care in certain circumstances.

When Your Health Information Can be Shared

- Under HIPAA, your health care provider may share your information face-to-face, over the phone, or in writing. A health care provider or health plan may share relevant information if:
- You give your provider or plan permission to share the information.
- You are present and do not object to sharing the information.
- You are not present, and the provider determines based on professional judgment that it's in your best interest.

Examples:

- An emergency room doctor may discuss your treatment in front of your friend when you ask your friend to come into the treatment room.
- Your hospital may discuss your bill with your daughter who is with you and has a question about the charges, if you do not object.
- Your doctor may discuss the drugs you need to take with your health aide who has come with you to your appointment.
- Your nurse may **not** discuss your condition with your brother if you tell her not to.
- HIPAA also allows health care providers to give prescription drugs, medical supplies, x-rays, and other health care items to a family member, friend, or other person you send to pick them up.

A health care provider or health plan may also share relevant information if you are not around or cannot give permission when a health care provider or plan representative believes, based on professional judgment, that sharing the information is in your best interest.

Examples:

- You had emergency surgery and are still unconscious. Your surgeon may tell your spouse about your condition, either in person or by phone, while you are unconscious.
- Your doctor may discuss your drugs with your caregiver who calls your doctor with a question about the right dosage.
- A doctor may **not** tell your friend about a past medical problem that is unrelated to your current condition.

For more information about sharing your health information with family members and friends, or more information about HIPAA, visit **www.hhs.gov/ocr/privacy/hipaa/understanding/index.html**.

For more information, visit **www.hhs.gov/ocr**.

U.S. Department of Health & Human Services
Office for Civil Rights

OFFICE FOR CIVIL RIGHTS

PRIVACY, SECURITY, AND ELECTRONIC HEALTH RECORDS

Your health care provider may be moving from paper records to electronic health records (EHRs) or may be using EHRs already. EHRs allow providers to use information more effectively to improve the quality and efficiency of your care, but EHRs will not change the privacy protections or security safeguards that apply to your health information.

EHRs and Your Health Information

EHRs are electronic versions of the paper charts in your doctor's or other health care provider's office. An EHR may include your medical history, notes, and other information about your health including your symptoms, diagnoses, medications, lab results, vital signs, immunizations, and reports from diagnostic tests such as x-rays.

Providers are working with other doctors, hospitals, and health plans to find ways to share that information. The information in EHRs can be shared with other organizations involved in your care if the computer systems are set up to talk to each other. Information in these records should only be shared for purposes authorized by law or by you.

You have privacy rights whether your information is stored as a paper record or stored in an electronic form. The same federal laws that already protect your health information also apply to information in EHRs.

Benefits of Having EHRs

Whether your health care provider is just beginning to switch from paper records to EHRs or is already using EHRs within the office, you will likely experience one or more of the following benefits:

- **Improved Quality of Care.** As your doctors begin to use EHRs and set up ways to securely share your health information with other providers, it will make it easier for everyone to work together to make sure you are getting the care you need. For example:
  - Information about your medications will be available in EHRs so that health care providers don't give you another medicine that might be harmful to you.
  - EHR systems are backed up like most computer systems, so if you are in an area affected by a disaster, like a hurricane, your health information can be retrieved.
  - EHRs can be available in an emergency. If you are in an accident and are unable to explain your health history, a hospital that has a system may be able to talk to your doctor's system. The hospital will get information about your medications, health issues, and tests, so decisions about your emergency care are faster and more informed.

- **More Efficient Care.** Doctors using EHRs may find it easier or faster to track your lab results and share progress with you. If your doctors' systems can share information, one doctor can see test results from another doctor, so the test doesn't always have to be repeated. Especially with x-rays and certain lab tests, this means you are at less risk from radiation and other side effects. When tests are not repeated unnecessarily, it also means you pay less for your health care in copayments and deductibles.
- **More Convenient Care.** EHRs can alert providers to contact you when it is time for certain screening tests. When doctors, pharmacies, labs, and other members of your health care team are able to share information, you may no longer have to fill out all the same forms over and over again, wait for paper records to be passed from one doctor to the other, or carry those records yourself.

Keeping Your Electronic Health Information Secure

Most of us feel that our health information is private and should be protected. The federal government put in place the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule to ensure you have rights over your own health information, no matter what form it is in. The government also created the HIPAA Security Rule to require specific protections to safeguard your electronic health information. A few possible measures that can be built in to EHR systems may include:

- "Access control" tools like passwords and PIN numbers, to help limit access to your information to authorized individuals.
- "Encrypting" your stored information. That means your health information cannot be read or understood except by those using a system that can "decrypt" it with a "key."
- An "audit trail" feature, which records who accessed your information, what changes were made and when.

Finally, federal law requires doctors, hospitals, and other health care providers to notify you of a "breach." The law also requires the health care provider to notify the Secretary of Health and Human Services. If a breach affects more than 500 residents of a state or jurisdiction, the health care provider must also notify prominent media outlets serving the state or jurisdiction. This requirement helps patients know if something has gone wrong with the protection of their information and helps keep providers accountable for EHR protection.

To learn more, visit **www.hhs.gov/ocr/privacy/**.

For more information, visit **www.hhs.gov/ocr**.

U.S. Department of Health & Human Services
Office for Civil Rights

OFFICE FOR CIVIL RIGHTS

YOUR HEALTH INFORMATION PRIVACY RIGHTS

Most of us feel that our health information is private and should be protected. That is why there is a federal law that sets rules for health care providers and health insurance companies about who can look at and receive our health information. This law, called the Health Insurance Portability and Accountability Act of 1996 (HIPAA), gives you rights over your health information, including the right to get a copy of your information, make sure it is correct, and know who has seen it.

Get It.

You can ask to see or get a copy of your medical record and other health information. If you want a copy, you may have to put your request in writing and pay for the cost of copying and mailing. In most cases, your copies must be given to you within 30 days.

Check It.

You can ask to change any wrong information in your file or add information to your file if you think something is missing or incomplete. For example, if you and your hospital agree that your file has the wrong result for a test, the hospital must change it. Even if the hospital believes the test result is correct, you still have the right to have your disagreement noted in your file. In most cases, the file should be updated within 60 days.

Know Who Has Seen It.

By law, your health information can be used and shared for specific reasons not directly related to your care, like making sure doctors give good care, making sure nursing homes are clean and safe, reporting when the flu is in your area, or reporting as required by state or federal law. In many of these cases, you can find out who has seen your health information. You can:

- **Learn how your health information is used and shared by your doctor or health insurer.** Generally, your health information cannot be used for purposes not directly related to your care without your permission. For example, your doctor cannot give it to your employer, or share it for things like marketing and advertising, without your written authorization. You probably received a notice telling you how your health information may be used on your first visit to a new health care provider or when you got new health insurance, but you can ask for another copy anytime.
- **Let your providers or health insurance companies know if there is information you do not want to share.** You can ask that your health information not be shared with certain people, groups, or companies. If you go to a clinic, for example, you can ask the doctor not to share your medical records with other doctors or nurses at the clinic. You can ask for other kinds of restrictions, but they do not always have to agree to do what you ask, particularly if it could affect your care. Finally, you can also ask your health care provider or pharmacy not to tell your health insurance company about care you receive or drugs you take, if you pay for the care or drugs in full and the provider or pharmacy does not need to get paid by your insurance company.

- **Ask to be reached somewhere other than home.** You can make reasonable requests to be contacted at different places or in a different way. For example, you can ask to have a nurse call you at your office instead of your home or to send mail to you in an envelope instead of on a postcard.

If you think your rights are being denied or your health information is not being protected, you have the right to file a complaint with your provider, health insurer, or the U.S. Department of Health and Human Services.

To learn more, visit **www.hhs.gov/ocr/privacy/**.

For more information, visit **www.hhs.gov/ocr**.

U.S. Department of Health & Human Services
Office for Civil Rights

THE MINIMUM NECESSARY REQUIREMENT
45 C.F.R. §§ 164.502(b) and 164.514(d)

Background

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

How the Rule Works

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. While guidance cannot anticipate every question or factual application of the minimum necessary standard to each specific industry context, where it would be generally helpful we will seek to provide additional clarification on this issue in the future. In addition, the Department will continue to monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the Rule does not hinder timely access to quality health care.

Uses and Disclosures of, and Requests for, Protected Health Information

For uses of protected health information, the covered entity's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access. For example, hospitals may implement policies that permit doctors, nurses, or others involved in treatment to have access to the entire medical record, as needed. Case-by-case review of each use is not required. Where the entire medical record is necessary, the covered entity's policies and procedures must state so explicitly and include a justification. For routine or recurring requests and disclosures, the policies and procedures may be standard protocols and must limit the protected health information disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request. Individual review of each disclosure or request is not required. For non-routine disclosures and requests, covered

entities must develop reasonable criteria for determining and limiting the disclosure or request to only the minimum amount of protected health information necessary to accomplish the purpose of a non-routine disclosure or request. Non-routine disclosures and requests must be reviewed on an individual basis in accordance with these criteria and limited accordingly. Of course, where protected health information is disclosed to, or requested by, health care providers for treatment purposes, the minimum necessary standard does not apply.

Reasonable Reliance

In certain circumstances, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- A public official or agency who states that the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the Rule, such as for public health purposes (45 CFR 164.512(b)).
- Another covered entity.
- A professional who is a workforce member or business associate of the covered entity holding the information and who states that the information requested is the minimum necessary for the stated purpose.
- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

The Rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

The Safe Medical Device Act Training Information

The Safe Medical Device Act (SMDA) is a law that was passed in 1990 and amended in 1992. It is regulated by the U.S. Food and Drug Administration (FDA). The SMDA requires home care agencies and other health care institutions to report to the FDA any incidents involving medical devices that are reasonably believed to have caused or contributed to the serious injury or death of a patient or employee. The intent of the law is to identify any medical device problems that pose a threat to public health and safety. Since serious injuries and deaths have occurred when a medical device has failed, has malfunctioned, was labeled incorrectly, and/or was used improperly, the SMDA seeks to identify 'bad' equipment in order that the public be protected from further harm.

A 'medical device' is any instrument, apparatus, machine, accessory to a machine, or similar related article that is used or intended for use in prevention, diagnosis, cure or treatment of a disease in man or animal or is used to affect the structure or function of the body of man or animals.

Some Medical devices used in home care may include:

A. Hospital beds
B. Wheelchairs
C. Oxygen Equipment
D. Ventilators
E. Walkers
F. Canes
G. Suction Equipment
H. Wound Vacs
I. Air Mattresses
J. Hoyer Lifts

Insulin pumps and infusion ports are considered medical devices, however the medication used in these devices is not covered under the act.

A 'serious injury' is one that:

A. Is life threatening
B. Results in permanent impairment or damage to a body structure or function
C. Necessitates medical or surgical intervention to prevent permanent impairment or damage

Staff Responsibilities regarding Medical Devices:

A. Agency staff should inspect the assistive equipment or medical devices that their patients are using on each visit.
B. Patients should be instructed not to use broken equipment until it is repaired or replaced. It is wise to place a tag or label on the piece of equipment that says "DEFECTIVE-DO NOT USE"
C. Equipment that is broken or not working properly should be reported to the medical equipment company so that it can be repaired or replaced.
D. Report your actions to your supervisor; document on your notes that you instructed the patient, tagged the equipment, called the equipment company, and notified your supervisor.
E. If you feel or learn that a medical device or piece of equipment has caused, or may have caused the death or serious injury of a patient, the following information must be reported to the office immediately so the FDA can be notified:
   - The patients name, address, etc.
   - A description of what happened to the patient
   - The manufacturer of the equipment and the identification of the device you believed caused the problem. Retrieve and report any model or product identification numbers that are visible on the device. Put aside and save, if you are able, the device, any packaging, and all required parts.
F. The Administrator will report to the FDA any event where a medical device is suspected as the cause of death in a patient.
G. An incident report will be completed.

Continuum's responsibility regarding the Safe Medical Device Act:

A. To report any event to the FDA where a medical device is suspected as a cause of patient death.
B. To keep detailed records according to the Agency's Safe Medical Device Act Policy.
C. To educate the staff annually regarding the requirements of the Safe Medical Device Act.

I, _____ acknowledge receipt of Medical Device Training materials. I further acknowledge that I have reviewed and understand the material provided to me, and agree to comply with the regulations set forth.

_____ _____

Signature **Date**

SAFE MEDICAL DEVICE ACT INSERVICE QUIZ

NAME: _____ **DATE:** _____

Select ALL correct answers.

1. Medical Device problems are tracked and monitored by:
   - ☐ The Social Security Administration
   - ☐ The FDA
   - ☐ Medicare

2. The Safe Medical Device Act is intended to:
   - ☐ Find ALL broken devices
   - ☐ Track how many manufacturers are selling defective medical devices
   - ☐ Identify any medical device that poses a threat to public health and safety

3. A Hoyer lift is a medical device.
   - ☐ True
   - ☐ False

4. A Wound Vac is a medical device.
   - ☐ True
   - ☐ False

5. Insulin is classified as a medical device.
   - ☐ True
   - ☐ False

6. A serious injury is NOT life threatening.
   - ☐ True
   - ☐ False

7. A serious injury causes permanent damage or injury.
   - ☐ True
   - ☐ False

8. If I find broken equipment patient's home, I should:
   - ☐ Call the FDA
   - ☐ Instruct the patient not use the defective equipment
   - ☐ Call the office to report the broken equipment to the supervisor

9. An incident report must be made out if a patient is injured from defective equipment.
   - ☐ True
   - ☐ False

10. Employee education on the Safe Medical Device Act must occur:
    - ☐ Every 5 years
    - ☐ Bi-annually
    - ☐ Annually

STANDARD PRECAUTIONS INFORMATION SHEET

Standard Precautions

What are Standard Precautions?
Standard precautions are a set of basic infection prevention practices intended to prevent transmission of infectious diseases from one person to another. Because we do not always know if a person has an infectious disease, standard precautions are applied to *every person every time* to assure that transmission of disease does not occur. These precautions were formerly known as "universal precautions.

Standard Precautions are the minimum infection prevention practices that apply to all patient care, regardless of suspected or confirmed infection status of the patient, in any setting where healthcare is delivered. These practices are designed to both protect HCP and prevent HCP from spreading infections among patients. Standard Precautions include: 1) hand hygiene, 2) use of personal protective equipment (e.g., gloves, gowns, masks), 3) safe injection practices, 4) safe handling of potentially contaminated equipment or surfaces in the patient environment, and 5) respiratory hygiene/cough etiquette.

Standard Precautions apply to 1) blood; 2) all body fluids, secretions, and excretions, *except sweat*, regardless of whether or not they contain visible blood; 3) non-intact skin; and 4) mucous membranes. Standard precautions are designed to reduce the risk of transmission of microorganisms from both recognized and unrecognized sources of infection in hospitals.

Standard precautions includes the use of: hand washing, appropriate personal protective equipment such as gloves, gowns, masks, whenever touching or exposure to patients' body fluids is anticipated.

AIDS

What is AIDS?
AIDS is a Bloodborne and sexually transmitted disease caused by a virus. The letters AIDS stand for Acquired Immune Deficiency Syndrome. When a person is infected with the Human Immunodeficiency Virus (HIV), the immune system is damaged. Without the body's natural defenses against disease, the person with AIDS is vulnerable to other infectious agents and can develop life-threatening illnesses such as pneumonia, cancer and meningitis.

How is AIDS transmitted?
AIDS is spread from one person to another during sexual contact, sharing of IV needles, and from an infected female to her unborn child. Contaminated blood products can also transmit the virus. HIV is spread through body fluids, primarily blood and semen.

Hepatitis B

What is Hepatitis B?
Hepatitis is an inflammation of the liver. Hepatitis B virus (HBV) presents a great risk to health care workers. Severe infections with HBV can be fatal. Chronic carriers of HBV may progress to liver cirrhosis, cancer, or death.

How is Hepatitis B transmitted?
Hepatitis B is spread from one person to another during sexual contact, sharing of IV needles, and from an infected female to her unborn child. Contaminated blood products can also transmit the virus.

Continuum
PEDIATRIC NURSING

DO'S AND DON'TS OF STANDARD PRECAUTIONS

1. **DO** wash your hands with soap, running water, and friction prior to patient contact, immediately following patient contact, between patients, and after removing gloves. Wash hands immediately after contact with any body fluids to which standard precaution apply. If hands are not visibly soiled, use of an alcohol-based hand rub may be used.

2. **DO** wear gloves when coming in contact with body fluids.

3. **DO** wear gloves when handling contaminated articles: lab specimens, dressings, linen, etc.

4. **DO** protect yourself from potentially infected materials by wearing gloves if you have any minor cuts, scratches, or dermatitis of the hands

5. **DO** wear masks, gowns, and/or goggles in addition to gloves, to protect yourself during procedures, which may involve the splashing body fluids.

6. **DO** prevent injuries from needles, scalpels, and other sharp instruments:
   DON'T recap used needles
   DON'T bend or break used needles
   DO place used disposable syringes, needles, and sharp items into a puncture-resistant container.

7. **DON'T** disregard an accidental needle stick or other exposure such as a splash to the eyes or mouth.
   DO cleanse the site thoroughly with soap and water, contact the nursing supervisor (if you are in the hospital or other facility) and notify the Director of Nursing immediately.

8. **DO** clean all blood and body fluids spills promptly. Use detergent and water followed by a disinfecting solution of 1 part household bleach to 10 parts water.

9. **DO** dispose of articles (used gloves, dressings, bandages, etc.) contaminated with blood or body fluids into a plastic bag. Close the bag tightly, place into a second plastic bag, and discard into a plastic lined trashcan.

10. **DO** treat all linen clothing soiled with blood or body fluids (to which standard precautions apply) as infectious.
    DO wear gloves and gown when removing such linen or clothing
    DO place the soiled articles into a plastic bag and later wash the articles in hot (160 degrees Fahrenheit) with detergent for 25 minutes.

Standard Precautions Quiz

Name: _____ Date: _____

1. AIDS is spread by sexual contact, sharing of needles, through infected blood and blood products, and from an infected female to her unborn child.
   - ☐ True
   - ☐ False

2. Health care workers are at risk for exposure to:
   - ☐ Hepatitis B virus
   - ☐ AIDS-Human Immunodeficiency virus
   - ☐ A and B

3. Standard Precautions apply to:
   - ☐ Blood
   - ☐ Non-intact skin
   - ☐ Mucous membranes
   - ☐ All body fluids, secretions and excretions, except sweat, regardless of whether or not they contain visible blood
   - ☐ All of the above

4. Standard Precautions include the use of: hand washing, appropriate personal protective equipment such as gloves, gowns, masks, whenever touching or exposure to patients' body fluids if anticipated.
   - ☐ True
   - ☐ False

5. Gloves should be worn when contact with the following is expected:
   - ☐ Mucous membranes
   - ☐ Blood
   - ☐ Non-intact skin or open wound
   - ☐ All of the above

6. Gowns should be worn whenever patient care activities might result in the health care provider's clothing coming in contact with blood, body fluids, or other contaminated articles.
   - ☐ True
   - ☐ False

7. Hand washing should be done:
   - ☐ Prior to patient contact
   - ☐ Immediately after you accidently have contact with blood and/or body substances
   - ☐ Immediately following patient contact and between patients
   - ☐ All of the above

8. The major risk of drawing blood or starting IVs is:
   - ☐ Blood Spills
   - ☐ Needle Stick Injury

9. To protect against needle stick injury:
   - ☐ Don't bend or break used needles
   - ☐ Don't recap used needles
   - ☐ Place all used needles and sharps in a puncture resistant container
   - ☐ All of the above

10. Gloves need not be changed before caring for the next patient.
    - ☐ True
    - ☐ False