YANKTON MEDICAL CLINIC®, P.C.

HIPAA Training

1. HIPAA – Health Insurance Portability and Accountability Act
    a. Passed 1996, enforced 2003, updated through the years.
    b. HITECH – Health Information Technology for Economic and Clinical Health Act – part of the American Recovery and Reinvestment Act of 2009 which gave incentives related to implementing and using electronic health records.
    c. HITECH widens the scope of privacy and security protections available under the original HIPAA rulings and gives specific guidelines health care providers and health plans must abide with.

2. HITECH provisions:
    a. Changes to our Notice of Privacy
        - Need an authorization for marketing purposes
        - Need to notify patients if their PHI has been disclosed inappropriately.
        - Document that patients have the right to withhold information from Healthcare Plans if they pay in full for services
        - No disclosure of genetic information may be made for insurance underwriting purposes.
    b. Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, requiring authorization.
    c. Business Associate agreement changes to make those companies follow HIPAA guidelines as well.
    d. Changes to the enforcement rules to incorporate increased and tiered civil money penalty structure provided by the HITECH act.
    e. Breach notification for unsecured protected health information under the HITECH act, replaces the breach notifications rule's harm threshold with a more objective standard. No longer is it necessary to show a patient experienced harm by the disclosure. Opens the door for litigation when a patients records are released in error, they no longer need to show damage….
    f. The Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes.
        - What this means for correspondence when we send records for new insurance applications, we cannot send out patient history forms patients fill out when seeing a new physician or specialist.
        - Insurance companies cannot use genetic information or basically family history of certain diseases.

3. Things to remember as you are working:
    a. No protected health information should be shared or discussed in open areas such as waiting rooms. Lab results, xray reports, diagnosis or referrals should never be discussed outside of an exam room.
    b. PHI includes patient name, date of birth, social security number along with the actual health information.

c. We cannot afford to make a mistake when working with a patient and their privacy. HITECH has taken out the harm clause so if a patient feels their information was disclosed inappropriately; they no longer need to prove they were harmed by it. Civil and criminal charges and fines are extensive and costly. Civil penalties can extend up to $250,000 with repeat or uncorrected violations, extending up to $1.5 million!
d. Our email system is not encrypted therefore not considered a secure connection so no patient information should be shared via email. That means within the clinic as well. If you need to share information regarding a patient, we need to use the NextGen tasking function. NextGen tasking is thru a secure network. If you don't know how to use it, check with a superuser. There is tasking in the EPM side as well as the EHR.
    - Blank forms are allowed to be transmitted via email, but completed ones are not.
    - If you receive information from outside the clinic regarding patients, ex. work comp or FMLA paperwork, do not email back regarding the patient. Phone calls or fax is the acceptable method.
    - If a teacher or other patient representative emails you something regarding a patient, do not reply via email.
e. Authenticating callers:
    - If a caller asks for information regarding themselves, always verify with date of birth, address, or another piece of information that will verify whom you are speaking to before giving out information.
    - If a caller is asking for information regarding another patient, we need to verify the caller has a right to that information, ex. DPR signed giving spouse authority to receive information.
    - If the caller claims to be from a law enforcement agency or DSS and there is no way to confirm they are who they claim to be. It is acceptable to ask for a number and call them back or ask for the request in writing on letterhead.
    - It is always best to error on the side of caution.
f. Leaving messages on phones
    - Do not leave PHI on voice mail or answering machines unless a patient has specifically asked you to and that is documented as a request or OK to leave a message.
    - Leave a message on voicemail or answering machine asking patient to return a phone call.
    - Confirming appointments - ?

4. Logging disclosures of PHI.
    a. HITECH and HIPAA requires health care providers to keep a log of any disclosures of protected health information. There was a proposed rule that would have required us to keep a log of each disclosure even for payment of a claim! Luckily that did not make it into the final ruling.

b. Each time we send medical records to another facility, we need to log that.
c. The patient has a right to a listing of disclosures, where his records have been sent or released to. NextGen has a PHI log built into the system. Each time PHI is sent out of YMC/VMC we need to document it.
d. PHI Log in the EHR:
    - Patient demographics tab at the top of the history bar, near the bottom (3rd from the bottom) is the PHI log.
    - Double click to open.
    - Double click or right click on the grid to add new.
    - Document the reason for disclosure, use the drop down pick list.
    - Date the request was made, who requested the disclosure.
    - Next section indicates what information is being disclosed.
    - Lower section has whom the information is being disclosed to and how, electronic, paper, or other. Medical records staff will indicate in the comments if records mailed, faxed and to what number faxed.
e. It is very important to log the disclosures, ex. We fax records to Lewis and Clark Behavioral as a referral. That facility sends our records on to the patients employer which is a hipaa violation if no signed authorization from the patient. The patient is let go from work due to something in his YMC note. Patient wants to know how the employer got those records. Without our record of disclosing to L & C Behavioral, there is no defense that we did not disclose the records inappropriately to the employer.
f. Each disclosure of medical records to another facility or entity outside the clinic must be documented. If providers or nurses do not want to take the time to document their disclosures, medical records will log it as long it is clear what information has been disclosed on the fax cover sheet.
g. Disability forms do not have to be logged, but the clinic notes, labs, rad reports, etc. do need to be logged.
h. The PHI log is a useful tool in seeing if or when records were disclosed.

5. Workstation and computer security
    a. Lock your computer when not in direct contact with your computer.
    b. Keep papers and computer secure, if you sit down at a common computer and the last use is still logged in, log them out before logging in with your log in and password.
    c. Keep your password confidential.

6. Security Committee has been formed and several policies have been documented and procedures will be introduced.
    a. Risk Analysis and Risk Management, in particular how we can protect patient's PHI and prevent breaches to our systems and keep patients confidential information safe.
    b. How Media is destroyed and a log of the destruction; ex hard drives from the computers, and CD's that have images of protected health information.
    c. Inventory, computer storage and back up of all the areas PHI is stored:

- EKG Machines
- DR System
- Orchard
- PFT machines
- NextGen

d. Auditing of all workforce.
    - Audits will look at what records have been accessed and look for trends in access.
    - Audits will be done randomly, and the goal will be to audit each staff member each year.
    - Audits will also be done as needed when investigating a suspected HIPAA violation.

7. Complaints of possible HIPAA violations will be fielded by the security officer and an investigation will be done with members of the security committee to determine if a violation or breach has occurred.
8. If a patient's record has been disclosed inappropriately or even accidentally to the wrong facility, we are required to inform the patient and log the disclosure.
9. Breaches of 500 + patients require us to inform state Department of Health and the media!! Ex. Laptop with unencrypted PHI from many many patients was stolen from a parking lot of a restaurant in Minneapolis. That was a costly error and received a lot of media coverage.
10. Confidentiality Agreement
    a. Disclose Patient Information and/or Confidential Information only if such disclosure complies with our policies and HIPAA and is required for the performance of my job.
    b. Keep log ins and passwords strictly confidential.
    c. Do not access or view any information other than what is required to do your job.
    d. Do not discuss any information pertaining to the clinic or patients in an area where others may hear.
    e. Do not discuss any clinic or patient information in public areas even if specifics such as a patient's name are not used.
    f. Do not make inquiries about any clinic or patient for anyone who does not have proper authorization.
    g. Do not make any unauthorized transmissions, copies, disclosures, inquiries, modifications, or purging of Patient Information or Confidential Information.
    h. Once you leave the clinic employment, you must return all clinic property, ex name badge, handbook, etc.
    i. Obligation under confidentiality agreement continues after you leave the clinic.
    j. Violation of the confidentiality agreement may result in disciplinary action, up to and including termination, as well as potential personal civil, and criminal legal penalties.
    k. Confidential Information or Patient Information that is accessed or viewed does not belong to me.
    l. Sign and date agreement – does not constitute a contract for employment.

YANKTON MEDICAL CLINIC®, P.C.

HIPAA Quiz

1. HIPAA is a federal law enacted to protect the privacy of a patient's personal and health information and provide for its physical and electronic security.
    a. The statement is TRUE
    b. The statement is FALSE
    c. HIPAA is NOT a federal law.
    d. HIPAA allows all healthcare workers to view patient records.

2. Who has to follow the HIPAA law?
    a. Physicians
    b. Physicians and all other patent care providers
    c. Only supervisors and other administrators
    d. All YMC workforce members

3. What does PHI mean?
    a. Physical health injuries
    b. Patient and hospital incidents
    c. Personal and health information
    d. Protected health information

4. Examples of Protected Health Information (PHI) include:
    a. Name, address, birthdate, SS#, email address
    b. Medical records, diagnosis, treatment, test results
    c. Billing records, research records, referral authorizations
    d. All of the above

5. Under what circumstances are you free to access and share PHI?
    a. Only if you know the patient won't mind
    b. After you no longer work at the organization
    c. After a patient dies
    d. Only if it is part of your job and can only be shared with individuals who need the information

6. Under HIPAA, patients have certain rights outlined in what document?
    a. Confidentiality Statement
    b. Notice of Privacy Practices
    c. Condition of Admission
    d. Information Release Form

7. Your sister's best friend has started cancer treatments at the clinic. Your sister asks you to find out her friends prognosis. What should you do?

a. Ask a nurse in the Chemo room how patient is doing and pass the information along to your sister.
b. Check the EHR for the oncology master and pass the information on to your sister.
c. Explain that it's a violation of the patient's privacy for you to ask around or look at her friend's record.
d. None of the above

8. When can YMC use or disclose PHI?
    a. For treatment of a patient.
    b. For payment of bills.
    c. When court ordered to.
    d. All of the above.

9. State and federal laws, as well as YMC clinic policy, require what form of patient information is to be protected and remain confidential?
    a. Written
    b. Spoken
    c. Electronic
    d. All of the Above

10. Because I have access to confidential patient information as part of my job, I can look up anybody's record, even if not for my specific work assignments, as long as I keep the information to myself.
    a. The statement is TRUE
    b. The statement is FALSE
    c. I can also share this information with my family and close friends as long as I know they won't pass the information on to others.
    d. I can access any paper medical records anytime, but not the electronic records.
    e. Both b and d.

11. You can protect patient information by:
    a. Protecting verbal or written information
    b. Utilizing safe computing skills
    c. Reporting suspected security incidents
    d. All of the above

12. A co-worker leaves her work station for a short time and leaves her PC logged in to the EHR. You need to look up information and sit down to use that computer, what should you do?
    a. Log your co-worker off and re-log in under your own User ID and Password.
    b. To save time, just continue working under your co-worker's user ID and password.
    c. Wait for co-worker to return before logging him or her out.
    d. Leave your co-workers computer logged on and find a different computer to use.

13. Accessing patient information electronically can be tracked back to your User ID and computer and identifies the documents viewed and activity done.
    a. The statement is TRUE
    b. The statement is FALSE
    c. User ID and computer cannot be tracked
    d. None of the above

14. I do not work with patients directly or have access to medical records, however, I see patients walk past my desk. I can tell family and friends who I see walking through the clinic as it is not sharing protected health information.
    a. The statement is TRUE
    b. The statement is FALSE
    c. I can't talk to family and friends, but I can talk to coworkers in the break room about whom I saw walk past.
    d. I can't discuss any patient information unless the information is needed to complete a task for my job.
    e. B and D
    f. B, C, and D

15. Which workstation security safeguard are YOU responsible for using and or protecting?
    a. User ID
    b. Password
    c. Logging out of programs that access PHI when not using them.
    d. All of the Above

_____
Print Name

_____ _____
Signature Date

_____ _____
Trainer Date

Note: This record may be included in the employee's personnel or training file.