2010

HIPAA Training

Glenn Cox
Fort Hays State University

HIPAA TRAINING

GBUS 674 Independent Studies

Glenn M. Cox

May 01, 2010

Table of Contents

SECTION 1---FORMAT

This is a training manual available to any organization that requires HIPAA training. The trainer will present material by lecture to the class. The lecture is supported by power point slides and informational hand outs. The lecture is an efficient method of training to communicate information to large numbers of trainees in the least amount of time. The lecture approach to training is less costly and can support other training methods. The audiovisual tool, a power point slide presentation, accompanies this lecture. This tool is popular with trainees and improves the communication skills of the trainer. The slides are numbered to correspond with a number noted in the lecture and will appear in the lecture script. This will enable the speaker to coordinate the lecture with the correct supporting power point slide.

I encourage the trainer to arrange chairs in the classroom into a semi-circle design so the audience will feel more comfortable with participation during answer and question periods (Noe, 2008). The training presentation is designed to last one hour and the trainer must be allow time to complete a posttest and post training satisfaction survey after the presentation. The trainer can offer prizes for participants who arrive on time or answer questions correctly.

SECTION 2---TRAINING OBJECTIVES

After the training, the participants will be able to answer the following:

List four examples of Protected Health Information.

Identify four rules for disclosure of Protected Health Information.

State three examples when authorization is not required to disclose Protected Health Information.

State the requirements of the Privacy Notice

Identify two penalties for violating HIPAA Privacy Rule.

SECTION 3---PHYSICAL RESOURCES

To provide this training you will need a room or space that can accommodate up two fifty people comfortably. The trainer should have pens, notepads, and handouts available for all participants. If a trainer is providing incentatives with games or prizes they should have these materials prepared and clearly instruct the participants on how they will be distributed. The trainer should place the chairs facing the speaker and the power point presentation screen. The trainer will need a power point slide projector for this presentation. The trainer will need to have adequate PA system to be heard by the audience (Hackett, Schumacher, & Winget, 1995).

SECTION 4---COSTS

This training presentation is available with power point slides, training manual, handouts, test and satisfaction surveys for $495.00. We do accept certified funds or a credit card.

SECTION 5---TARGET AUDIENCE

- All key members of a health care provider privacy compliance team
- Compliance team for HIPAA Privacy
- Business associate Privacy compliance officer
- Professionals servicing Healthcare Industry
- Healthcare executives
- Healthcare service bureau executives
- Lawyers involved in healthcare
- HIPAA Privacy Compliance officers
- Pharmaceutical company executives and HIPAA compliance staff
- Insurance executives
- Clinical physicians and office managers
- Healthcare quality assurance and risk managers
- Clinical trial organization executives
- Business Associates to covered entities (HIPPA Training.Net, 2010)

SECTION 6---LESSON PLAN

Course title: HIPAA Training Manual

Lesson title: Know your HIPAA

Session duration: One hour for training, twenty minutes for post training test and survey.

Learning Objectives:

List four examples of Protected Health Information.

Identify four rules for disclosure of Protected Health Information.

State three examples when authorization is not required to disclose Protected Health Information.

State the requirements of the Privacy Notice

Identify two penalties for violating HIPPA Privacy Rule.

Audience: Employees who work with Protected Health Information.

Prerequisites: Participants should know job essential functions. The Instructor should be able to speak in front of large groups and understand HIPPA rules.

Room arrangement: Chairs and space for up to fifty participants.

Materials: Power point projector, hand outs, pens/pencils, notepads, prizes, test and evaluations.

Assignments: Post test and training evaluation.

Lesson outline	**Instructor Activity**	**Trainee Activity**	**Time**
Introduction	Present	Listen	10 minutes
Lecture	Present/question	Watch, answer	50 minutes
Test	Observe/collect	Write	10 minutes
Evaluation	Observe/collect	Write	10 minutes

SECTION 7---PRESENTATION

TRAINER PREPARATION:

In preparation for each training session, the trainer should align the chairs in the room to face the speaking and presentation area. I encourage a chair placement design the gives more space to the audience and presenter such as a half circle or horseshoe. To encourage learning atmosphere offer door prizes to the first ten participants that enters the room. The trainer can additionally obtain prizes and distribute them to participants who answer questions during the training presentation. The prizes can be any item that is affordable and easy to hand out without disrupting the focus of the audience. At the entry points of the room place signs with instructions informing the participants of items they should acquire as they enter the room. This is where the handouts, post test, evaluations, pens, pencils, notepads can be placed on tables that are easily accessible to the participants.

The presenter should turn on the power point projector and become familiar with the operation of the machine by reviewing a few of the slides. Remember to leave on the projector and to check the training script as the lecture will be supported with corresponding power point slides that are numbered. The trainer should be familiar with lecture portion of the presentation, test, and evaluations prior to the presentation.

The trainer is welcome to change any format arrangement to suit their needs or the needs of the participants. An effective presentation is will increase the training value that will assist the participants with improving their work skills. The trainer should plan additional activities if they are not satisfied with the question and answer periods included in this training presentation. The trainer should be comfortable in front of the audience and be entertaining when possible. The

trainer should be familiar with the process and outcomes of the training materials. Finally, the trainer will need to certain the audience understands the material and collect all relevant feedback, the test, and evaluations, from the participants (Businessballs.com, 2010).

TRAINER ACTIVITY:

When you begin each training session and as participants are entering the room designated for the training session remind them to take hand outs from stakes of materials located near the entry points. You can also hand out these materials and greet participants as they entry the training room. The participant should have note taking ability, hand out, training evaluation and sign any attendance sheet that is required by the sponsor organization. Encourage participants to locate a seat and become comfortable. After participants are seated and entry doors are closed, begin training with introduction.

TRAINER INTRODUCTION:

Slide 1, "Thank you for attending this training on Health Insurance Portability and Accountability Act, or fondly referred to as HIPAA. In this training you will listen to an interactive lecture as I will stop for question and answer periods throughout this training. There will be an test after the training so please take notes and ask questions as we review the materials. If you do not pass the test with ninety percent accuracy there will be an opportunity to take the test again. Everyone in this room should have signed an attendance sheet that is required by your employer. You should also have a hand out and a training evaluation, if you have not signed the attendance or have the other items please get them now or sign the sheet before we start. If you do not have writing, material please get hose now and everything you need is located on tables by the doors of the room. There are a few housekeeping rules requested

management that you remove your trash after the training is complete. If anyone must use a restroom during training, please do so as this session will be one hour long and another thirty minutes to complete test and evaluation. Please turn off your cell phones or any non-essential electronic devices that you may have with you. Relax enjoy the presentation raise your hand with questions at any time and remember we will have open period for questions and answers. Now let us get started with finding out about HIPAA and your responsibilities".

TRAINER ACTIVITY:

Please note the lecture has corresponding power point slides and as you share the lecture with the participants remember to align your lecture slide number with the number on the power point screen. Do not include citations when reading the lecture script.

TRAINER LECTURE:

Slide 2 , "HIPAA or the Health Insurance Portability and Accountability Act is intended to protect health information for employees and patients of medical facilities. There are four intentional focus areas of the law. The law is to limit the ability for exclusions in coverage under a new employer health plan for pre-existing conditions. The law provides additional opportunities to enroll in a health plan if you lose coverage or experienced certain life events such as pregnancy. The law prohibits discrimination against employee or their family members based on medical history or prior medical treatments, prior claims or generic information. Finally, the law guarantees that certain individuals can access and renew existing medical insurance policies" (United States Department of Labor, 2010).

Slide 3 , "Remember the law is to protect your health insurance information as it relates to five areas. The information you discuss with your doctors and other health care providers is

protected. Conversation regarding your health care treatment and information in the covered entities billing system or computer is protected. Finally, most health information held by your employer or medical provider network is protected health information or PHI" (Health and Human Services, 1996).

Lecture continued, "The PHI identification must be kept private and there are 18 identifiers that fall under HIPAA Privacy Rule. The name, address, phone number, social security number, fax number, email address and license number are a few of these identifiers, Slide 4, take a moment to look at this slide to note the remainder of the identifiers" (University of California, 2008). Slide 5, "In review Protected Health Information, called PHI, means any health information, including demographic information, whether it is oral, recorded, electronic or any other information medium. This applies to information received or created by a health care provider, under a health plan, an employer or a health care clearinghouse" (U.S. Department of Health and Human Services, 2010).

Lecture continued, Slide 6, "The HIPAA Privacy Rules address's what information must be protected by the covered entities. The HIPAA security rules provide guidelines of how information should be protected. The covered entities, health care providers, health plan administrators, health clearinghouses are required to enforce policy and procedures to secure your private health information. You received a handout when you entered the room that list covered entities. Slide 7, These processes can be safeguards such as locked storage files, conversation procedures such as requiring private rooms to review PHI. There must be a time limit on consent of sharing PHI with other approved parties and the minimum amount of information necessary is required. The security rule requires all contractors follow the same privacy and security rules of the covered entity. Finally the security rules place limits of access

on who can review health information and implement training programs for employees on how to protect health information" (U.S. Department of Health and Human Services, 2010).

TRAINER ACTIVITY:

Stop lecture and begin a period of question and answers. Read the following questions and ask the audience for an answer or ask an individual participant. Do not pressure anyone to answer, this is now a good time to share prizes for anyone who chooses to answer if you have chosen this format. The answer to each question follows the question, make certain the audience hears the correct answer.

Q. What does the law required to protect health information?

A. Health information that identifies you is kept private, you have rights enacted with the management of your health information, you receive legal notice regarding privacy practices, and all privacy practices that affect you are followed.

Q. What is a covered entity?

A. Health care provider, health insurance plan, health care clearinghouse.

Q. Name four identifiers that are related to Protected Health Information.

A. There are eighteen identifiers, the most common listed are name, address, email address, phone number.

TRAINER LECTURE:

Slide 8, "Now many of you attending today work for a covered entity and will need to learn the exact policy your employer has developed to address HIPAA. An employer may not be a

covered entity however, they will request information from covered entity. If your employer administers your health care plan, they are a covered entity. They should then have HIPAA policy to address the requirements of the law. I am going to share a summary I found on the Texas Department of Health website. Remember a covered entity must adopt written PHI privacy procedures; designate a privacy officer; require their business associates to sign agreements respecting the confidentiality of PHI; train all of their employees in privacy rule requirements; give patients written notice of the covered entities' privacy practices and access to their medical records; a chance to request modifications to the records; a chance to request restrictions on the use or disclosure of their information; a chance to request an accounting of any use to which the PHI has been put; and a chance to request alternative methods of communicating information. They must also establish a process for patients to use in filing complaints and for dealing with complaints. Finally, they must take any measures necessary to see that PHI is not used for making employment or benefits decisions, marketing, or fundraising" (U.S. Department Health and Human Services, 2003).

Lecture continued, "This is a very good summarization of the responsibilities for covered entities and many of you here today are likely employed by a covered enmity. Please note the key points, the first is a privacy officer, this is someone who is responsible at your organization to implement and monitor HIPAA policy. Employees and agents of the organization are required to sign privacy agreements that indicate how much PHI they can access without further consent. All releases must be offered in alternative methods of communication for those who may be impaired by communication disorders. Your organization must offer a formal system to file a complaint when HIPAA standards are possibly violated and they must ensure PHI is not used for

business decisions affecting an individual based on the individual's health status" (UTMB, 2002).

TRAINER ACTIVITY:

Now stop lecture and announce to the class you will read the following scenario. After you have the read the scenario please ask the participants to share their opinion.

TRAINER EXERCISE:

" I am now going to share a HIPAA situation that actually happened and after I am finished I will ask you to share your opinions on this scenario. I will want to know if you think this was a HIPAA violation or not a violation." Here is the scenario:

My husband works in a teaching hospital doing EEGs. Sometimes something on an EEG will indicate a brain lesion that could be confirmed by seeing an MRI. My husband was told by his manager that it was allowed and acceptable to look at a patient's imaging for educational purposes. So he had a patient that he performed several EEG's on, saw something that indicated a brain lesion and looked at the patients MRI to confirm. Now his manager's supervisor is trying to charge him with violating HIPAA. It just doesn't seem right. His manager gave him consent to look at imaging and MRIs are very closely related to EEGs. Also he was looking at the EEG of his own patient. To top it off his Supervisor told him that ordinarily it wouldn't matter but the patient just happened to be a high profile patient. So famous people are entitled to more privacy than the rest of us? It just seems wrong to me. Also if looking at that imaging was a HIPAA violation, how does his manager giving him the okay to do that effect any disciplinary action he might receive? If his behavior was inappropriate he was only doing what he had been instructed

was ok to do, and any breach of HIPAA would have been a complete accident" (Yahoo Answers, 2010).

TRAINER ACTIVITY:

Now stop and ask participants their opinion, allow a few minutes hand out prizes if you wish to those who become involved in the discussion, and then read the following answer:

Lecture continued, "Thank you all for sharing and here was the answer that was posted: That is not a violation of HIPAA. Your husband was hired to do EEGs. He ran an EEG on a patient. What else is your husband supposed to do besides read the EEG? How can a doctor treat a patient without looking at the test results? This is in no way a HIPAA violation. However, it could be a hospital policy violation, and there is nothing that prohibits an employer reprimanding an employee for violating company policy. Perhaps the hospital requires third parties to read EEGs, or something like that, and your husband was prohibited from viewing the EEG on that basis (Ibid, 2010).

TRAINER LECTURE:

"So you have organizational process's to consider in this scenario as it was a liability issue and not an HIPAA violation. Remember, it is important to remember there are penalty's for violating HIPAA requirements that are separate from outcomes of a liability situation. In this scenario, a patient has every right to know their PHI however, the provider has to consider the liability exposure of a diagnosis by the technician. You will need to be certain you understand your organizations policies for all information sharing."

Lecture continued, Slide 9, "Now there is PHI your organization can share without consent when certain conditions apply. Health information can be used or disclosed to facilitate medical treatment or services by providers. The health information can be share with doctors, nurses, technicians, medical students or other involved personnel assisting in your care. One example is information about you after an injury has occurred at work. Health information can be disclosed or used without consent for the purpose of payment to providers for you health care or services. This also includes to determine the benefit responsibility of a patient's plan or to coordinate the health care plan coverage. An example could be sharing medical history to determine the correct billing code or to determine if the health plan will cover the procedure. Health information can be disclosed without consent for other health care operations such as conducting quality assessment or improvement activities. There are additional reasons it could be disclosed such as submitting claims for stop-loss coverage, medical reviews, legal services, audit services and fraud or abuse detection programs. Remember there are situations when health information can be disclosed without consent and you will need to check your organization's policies to find out what is allowed by your organization" (HIPPA Training.Net, 2010).

TRAINER LECTURE:

Slide 10, "Now what happens if there is a violation of HIPAA and your organization does not effectively address the issue I have found a nice summary from the American Medical Association website that I will review with you. This is also a handout. This is recent civil and criminal penalties for HIPAA violations and legislated in the "American Recovery and Reinvestment Act" (ARRA), of 2009. The Secretary of the Department of Health and Human Services (HHS) still has discretion in determining the amount of the penalty based on the nature

and extent of the violation and the nature and extent of the harm resulting from the violation. The Secretary is still prohibited from imposing civil penalties (except in cases of willful neglect) if the violation is corrected within 30 days (this time period may be extended).

Lecture continued, "The criminal penalties for a violation of HIPAA are directly applicable to covered entities—including health plans, health care clearinghouses, health care providers who transmit claims in electronic form, and Medicare prescription drug card sponsors. Individuals such as directors, employees, or officers of the covered entity, where the covered entity is not an individual, may also be directly criminally liable under HIPAA in accordance with principles of "corporate criminal liability." Where an individual of a covered entity is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting. The goal is how to interpret the "knowingly" element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required (American Medical Assoication, 2010). Now you can note the fines on your handout or write them down from the power point slide. Remember there are consequences for not adhering to HIPAA policy and law. "

TRAINER ACTIVITY:

Stop and inform the audience you are going ask questions and invited anyone to answer, plus you may offer prizes to those who answer. Be certain to share the correct answers with the participants.

Q. What health information be released without consent under HIPAA?

A. Information for treatment, payment and health care operations.

Q. Are there consequences for not complying with HIPAA?

A. Yes there are fines, penalties, and criminal prosecution

TRAINER LECTURE:

" Now there are other disclosures I want to review with you. HIPAA allows required disclosures to the individual when they request their health information. Slide 11, This includes billing statements and other information used to determine health care decisions. This also includes an accounting of health information released to other parties that are authorized by the individual to receive the information. Remember an individual will sign consents and authorizations that can include a personal representative for that individual. The individual can revoke this authorization anytime in writing. There are other directions with health information the individual may request such as restriction on who can receive their health information. They may request family members not receive health information or a friend, remember it is the choice of the individual. The individual can request information or communication is transmitted or sent to one specific location. This can be an email address or a P.O. Box address, once the request is submitted in writing the provider must comply. Individual can request to inspect health information that has been used to make decisions about their health coverage or benefits. Indivudals can request to amend any authorizations or health care information that is incomplete or incorrect as perceived by that individual. The individual can request an accounting of parties that have received health care information about them by their health care provider or the covered entity associated with the individual. Finally, the individual can and should receive a copy of the HIPAA privacy notices and the individual's reception of the notice should be documented. Remember to make certain indivudals have signed they received a copy of the notice and practices affecting their health information" (Chicago Department of Public Health, 2005).

TRAINER ACTIVITY:

Now stop lecture and prepare to ask questions, remember to make certain the participants hear the correct answer. Ask questions and solicit response from participants.

Q. What is included in the individual authorization?

A. Description of PHI to be disclosed, who will use the PHI and for what purpose, whether or not there is financial gain will result from disclosure for other HIPAA organization, signature or their representative, an expiration date (National Institutes on Health, 2004).

Q. Can an individual withdraw consent or restrict who received PHI?

A. Yes, they can put in writing withdrawal of authorization or limit who receives PHI on the authorization.

TRAINER LECTURE:

Slide 12, "Now to summarize before we finish the lecture and you all begin your test. HIPAA is a law that protects health information of indivudals. Protected Health information is identifying information that relates to an individual's past, present and future health care, or mental health care. This can be information that indentifies current medical conditions of the individual. The information where there is reason to believe the share information can identify the individual and is created or received by health care providers or covered entities. There are penalties for not complying and criminal prosecution in some cases for HIPAA violations. You as employer must ensure authorizations are signed and dated properly and make certain all individuals have copies of the privacy rules and security measures required by HIPAA (PARTNERS Human Research Committee, 2003). Slide 13, This is not all you will need to

know I encourage everyone to check with you organization privacy officer or HIPAA committee when you return to your place of employment for specific policies, remember the case of liability versus HIPAA. Now are there any final questions?"

TRAINER ACTIVITY:

Now answer any questions and then inform participants they can take the test and to complete the training evaluation. Stay at the front of the room to answer questions or give direction. Ask participants to leave test and evaluations at a place you can find them. After participants have left and the room is empty organize the room for the next training and grade test. After the grading is completed, send results to appropriate recipient such as the individual or the employers that sent employees to the training. This information will be listed in the training registration.

SECTION 8---EVALUATIONS

Participants are expected to complete a eighteen question test after the training session and score ninety percent to receive a certificate of completion. Only two attempts to pass the test will be offered and afterwards scoring less than ninety percent will require the participant to repeat the training. There is a training evaluation that will be completed by participants and the evaluation scores should rate eighty percent in the areas of fair, good, or great categories. The test, test answers, and training evaluation are listed in the table of contents. Participants may refer to hand outs while completing the test.

SECTION 9---TRAINING ANNOUNCEMENT AND REGISTRATION

ANNOUNCEMENT

HIPAA TRAINING

DOOR PRIZES

HERE FOR ONE DAY

Wednesday

1:00 P.M.

Large Training Room

Be sure to complete registration below if you want to be hip on HIPAA

NAME:

TITLE:

AGENCY:

ADDRESS:

WORK PHONE:

CELL PHONE:

EMAIL:

SEND TRAINING CERTIFICATE TO:

Please include your $25.00 non-refundable registration fee. Please specify who should receive your Certification of Training or if you and your employee will need a copy. Please complete the registration with your name formatted the same way you wish it to be shown on your Training Certificate.

TEST

CIRCLE THE CORRECT ANSWER

NAME:

1. Which of the following is considered Protected Health Information?

A. A physical report from your physician.

B. A medical file with your name and address.

C. An email address listed on a computer screen of a health care provider.

D. All of the above.

2. Which of the following is required when disclosing Protected Health Information?

A. Minimum amount of information necessary.

B. Authorized by the individual.

C. A listing of specific information to be disclosed and the reason.

D. All of the above.

3. Protected Health Information can be disclosed without consent for the purpose of:

A. Payment of health care operations.

B. To the individual.

C. For emergency health services.

D. All of the above.

4. The HIPAA Privacy Rule protects an individual's right to privacy.

A. True

B. False

5. You are permitted to disclose PHI to a third party with written authorization for the individual or their personal representative.

A. True

B. False

6. PHI stands for Protected Health Information.

A. True

B. False

7. An individual can restrict who receives PHI.

A. True

B. False

8. The HIPAA Privacy Rule allows individuals to complain if their privacy is violated.

A. True

B. False

9. If an individual believes their privacy has been violated they should notify:

A. The Privacy Officer.

B. A co-worker.

C. A supervisor.

D. A spouse.

10. Protected Health Information is anything that connects a person to their health information?

A. True.

B. False.

11. An authorization must contain an expiration date.

A. True.

B. False.

12. After an authorization is received the individual or their representative can revoke it.

A. True.

B. False.

13. You can be fined $100.00 for a HIPAA violation.

A. True.

B. False.

14. A covered entity is required to implement all HIPAA regulations.

A. True.

B. False.

C. Neither.

15. Your employer is a covered entity if they:

A. Offer you medical insurance.

B. Are involved with providing health care services.

C. Administer a self-insured medical plan.

D. B & C.

16. A social security number and a driver license number are considered PHI.

A. True.

B. False.

17. An individual can request to see who has received their PHI.

A. True.

B. False.

18. The maximum fines for HIPAA violations in a one-year period are:

A. $25,000.

B. $250,000.

C. $500,000.

D. A & B.

TEST ANSWERS

1. D
2. D
3. D
4. A
5. A
6. A
7. A
8. A
9. A
10. A
11. A
12. A
13. A
14. A
15. D
16. A
17. A
18. D

TRAINING EVALUATION

From the scale rate items listed below: 1-pointless, 2-poor, 3-fair, 4-good, 5-great

Room was comfortable and chairs where easy to find ____

Materials for writing and taking notes where available ____

Instructions were easy to follow ____

Presentation was informative ____

Speaker was knowledgeable ____

Training was useful ____

Video and audio where clear ___

Allowed time was sufficient ___

Subject was relevant ___

COMMENTS:

HAND OUT

HIPAA VIOLATIONS AND FINES

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 $50,000per violation, with an annual maximum of $1.5 million $50,000 per violation, with an annual maximum of $1.5 million

Criminal Penalties

In June 2005, the U.S. Department of Justice (DOJ) clarified who can be held criminally liable under HIPAA. Covered entities and specified individuals, as explained below, whom "knowingly" obtain or disclose individually identifiable health information in violation of the Administrative Simplification Regulations face a fine of up to $50,000, as well as imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Finally, offenses committed with the intent to sell, answer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years (American Medical Assoication, 2010).

HAND OUT

COVERED ENTITY

1. **Health care providers** are covered if they transmit health information *electronically.* Even a doctor in a small practice who keeps only paper records will almost certainly use a billing service that transmits information electronically. In short, it is nearly impossible to provide health care today without using electronic means in some way.

   As long as information is transmitted electronically, "health care provider" includes your doctors, hospitals, staff involved in your treatment, laboratories, pharmacists, dentists, and many others that provide medical, dental, and mental health care or treatment. In short, a provider is almost anyone in the business of providing health care who is licensed or regulated by the states.

2. **Health plan** means almost anyone that pays for the cost of medical care. This includes: health insurance companies, HMOs (health maintenance organizations), group health plans sponsored by your employer, Medicare and Medicaid, and virtually any other company or arrangement that pays for your health care.

3. **Health care clearinghouses** can be any number of organizations that work as a go-between for health care providers and health plans. An example of this would be a billing service that takes information from a doctor and puts it into a standard coded format. Patients rarely deal directly with clearinghouses.

An organization may also be what is called a **hybrid entity**. A hybrid entity provides health care as *only part* of its business. A large corporation that has a self-insured health plan for its employees is one example of a hybrid entity. Only the portion of the company that processes claims and makes payments to health care providers is subject to the HIPAA Privacy Rule.

Your medical information may be available to many who are *not* covered by HIPAA. Here are some examples of who is *not* covered.

- Life insurance companies.
- Workers Compensation.
- Agencies that deliver Social Security and welfare benefits.
- Automobile insurance plans that include health benefits.
- Internet self-help sites.
- Those who collect health data you give voluntarily for surveys or research projects.
- Those who conduct screenings at pharmacies, shopping centers, hometown fairs, or other public places for blood pressure, cholesterol, spinal alignment, and so on.
- Researchers who obtain health data directly from health care providers.
- Law enforcement agencies.

Even though these organizations are not covered by HIPAA, they may get information from a covered entity (Privacy Rights Clearinghouse, 2010).

HAND OUT

HIPAA IDENTIFIERS

1. Names
2. ALL geographic subdivisions smaller than the state
3. All elements of dates smaller than a year (i.e. birth date, admission, discharge, death, etc.)
4. Phone numbers
5. Fax numbers
6. E-mail addresses
7. SS numbers
8. Medical record number
9. Health plan beneficiary
10. Any other account numbers
11. Certificate/license numbers
12. Vehicle identifiers
13. Device identification numbers
14. WEB URL's
15. Internet IP address numbers
16. Biometric identifiers (fingerprint, voice prints, retina scan, etc)
17. Full face photographs or comparable images
18. Any other unique number, characteristic or code (University of Vermont, 2010).

HANDOUT

AUTHORIZATION

The general rule is that a covered entity may not use or disclose PHI without an individual's written authorization, except if permitted or required by the Privacy Rule. Individuals have several rights that the covered entities must protect.

- **Notice of Privacy Practices and Written Acknowledgement:** Covered entities (including health care providers) must give individuals an understandable notice of the ways in which PHI will be used and disclosed. "Use" means sharing within the Partners system, and "disclose" means releasing outside of the system. Entities must make a good faith effort to obtain a written acknowledgement of receipt of the notice.

- **Uses and Disclosures of Protected Information**

    - **Authorization:** Authorization is required for several uses and disclosures of PHI. One example is for research; generally, a researcher must obtain a subject's authorization before using or disclosing PHI for a study, unless the researcher obtains an IRB-approved waiver of authorization.
    - **Oral Agreement or Objection:** If a covered entity wants to include PHI in a facility directory, disclose it to clergy, or disclose it to family or close friends of the patient, it does not need the patient's written authorization. It must, however, give the patient a reasonable opportunity to opt in or opt out.

- **Minimum Necessary Standard:** When a covered entity uses or discloses PHI or requests it from another covered entity, the entity generally must try to limit such information to the "minimum necessary" needed to achieve the purpose. The entity must adopt policies that address what information generally meets this standard for uses, requests, and routine disclosures. For non-routine requests and disclosures, criteria must be developed to permit case-by-case review of the minimum necessary for each purpose. Importantly, the minimum necessary standard does not apply to treatment-related disclosures made to facilitate treatment (e.g., a hospital may release a copy of a full record to an outside physician providing a second opinion). The minimum necessary standard also does not apply when an individual has authorized the use or disclosure (e.g., if a person enrolls in a study and authorizes use and disclosure of her PHI for that purpose, then the researchers do not need to determine what is the minimum necessary information they may use or disclose for the research).

Individual Rights and Entity Responsibilities

- **Notice, Authorization, and Revocation:** Covered entities must give individuals a notice of privacy practices, try in good faith to obtain a written acknowledgement of receipt of the notice, and obtain authorizations when applicable. Individuals have a right to revoke the authorization except to the extent an entity has relied on it. In the event an individual refuses to sign or

revokes an authorization, the entity must have mechanisms to track those decisions and ensure they are followed.

- **Access:** Individuals generally have a right of access to their PHI. A covered entity may charge a reasonable fee for copying and postage.
- **Amendment:** Individuals have a right to amend their PHI. If the entity approves the request, it must inform the individual; persons or entities the individual identifies as needing the amendment; and others, including business associates, who may have relied or could rely on such information to the individual's detriment.
- **Accounting of Disclosures:** Individuals have a right to request a list of disclosures of their PHI. The list generally must indicate how, when, why, to whom, and to what extent their PHI has been disclosed outside the covered entity over the previous six years. This right does not include disclosures for treatment, payment, and health care operations, disclosures authorized by the individual, disclosures for certain law enforcement and other purposes, or disclosures occurring before the effective date of the rule. To comply with this requirement, a covered entity will need to ensure not only that it has personnel to review and respond to these requests, but more critically, that it has information systems or other mechanisms to track individual disclosures and their circumstances as they occur. Note that an alternative tracking approach is available for some research (as indicated below).
- **Request for Restrictions:** Individuals may ask a covered entity to restrict its uses or disclosures of their PHI, but the entity need not agree to the restriction. In such a situation, if the individual does not accept the protections that can be provided, the individual can decide to obtain care elsewhere.
- **Confidential Communications:** Individuals may ask that a health care provider communicate with them by alternative means or at an alternative location (e.g., home vs. office, mail vs. email). A provider must reasonably accommodate the request and may not require an explanation.
- **Personal Representatives:** Although not described as an individual right, a covered entity must treat individuals' family and other "personal representatives" in the same way as the individuals, with certain exceptions. Personal representatives include not only family (including parents of minors), but also other relatives, close personal friends, or others who are authorized to act for an individual with respect to decisions concerning health care treatment or payment. An entity has discretion not to treat someone as a personal representative if it reasonably believes an abusive situation exists, the individual may be harmed, or it is otherwise not in the individual's best interest.
- **Deceased Individuals:** A covered entity must protect the privacy of a decedent's PHI for as long as it maintains the information. This in part reflects the ongoing sensitivity of genetic and hereditary information. A personal representative (e.g., an executor) may access PHI, as may a provider for purposes of treating other family members. In addition, a decedent's PHI may be used for certain research purposes without an authorization (PARTNERS Human Research Committee, 2003).

REFERENCES

U.S. Department Health and Human Services. (2003, April). *HIPAA PRIVACY RULE-WHAT EMPLOYERS NEED TO KNOW.* Retrieved April 2, 2010, from HIPAA privacy rules-what employers need to know: http://www.twc.state.tx.us/news/efte/hipaa_basics.hmtl.

AMA. (2010). *Frequently asked questions about the HIPPA privacy*. Retrieved February 24, 2010, from AMA American Medical Association: http://www.ama-assn.org/ama/pub/physician-resources.

American Medical Assoication. (2010). *HIPAA Violations and enforcement.* Retrieved March 15, 2010, from AMA: http://ama-assn.org/ama/pub/physician-resources/solutions/hippahealth-insurance.

Businessballs.com. (2010). *Businessballs.com*. Retrieved March 31, 2010, from presentation skills: http://www.businessballs.com/presentation.htm.

Chicago Department of Public Health. (2005, April 20). *HIPPA 100 Training Manual.* Retrieved Febraury 16, 2010, from HIPPA Training Manual: http://www.uic.edu/nursing/forms/Clinical_Site_Requirements/CDPA/HIPPA.

Dea MD, R., Cooper MD, T., & Cohen MD, S. (2003). *HIPPA: What's True, What Isn't*. Retrieved March 3, 2010, from The Permanente Journal: http://xnet.kp.org/permanentejournal/03/hippa.hmtl.

Hackett, D. D., Schumacher, L., & Winget, R. (1995). *Train the Trainer.* Wichita Kansas: Wichita State Universtiy.

Health and Human Services. (1996, August 21). *Public Law Health Insurance Poertability and Accountability Act of 1996.* Retrieved March 21, 2010, from ASPE Health and Human Services: http:aspe.hhs.gov/admnsimp/p104191.htm.

HIPPA Training.Net. (2010). *HIPPA Training and Compliance Solutions*. Retrieved March 15, 2010, from HIPPA TRAINING.NET: http://www.hippatraining.net/index.hmtl.

HIPPA.ORG. (2003). *Unsure how to handle HIPPA?* Retrieved February 24, 2010, from HIPPA.ORG: www.hippa.org/.

National Institutes on Health. (2004, July 4). *HIPAA Authorization for Research*. Retrieved April 8, 2010, from National Institutes on Health HIPAA Privacy Rule: http://privacyruleandsearch.nih.gov/authorization.

Noe, R. A. (2008). *Employee Training and Development.* New York: McGraw-Hill Irwin.

PARTNERS Human Research Committee. (2003, April 14). *Overview of the HIPAA Final Privacy Regulations*. Retrieved April 9, 2010, from PARTNERS Human Research Committee: http://healthcare.partners.org/phsirb/hipaaov.htm.

Privacy Rights Clearinghouse. (2010, Janauary). *HIPAA Basics Medical Privacy in Electronic Age*. Retrieved April 7, 2010, from Privacy Rights Clearinghouse Empowering Consumers, Protecting Privacy: http://www.privacyrights.org/fs/fs8-hippa/htm#3.

Privacy Rights Clearinghouse. (2010, January). *Medical Privacy in Electronic Age*. Retrieved March 25, 2010, from Privacy Rights Clearinghouse: http://www.privacyrights.org/fs/fs8-hippa.htm.

SearchSecurity.com. (2009, April 13). *HIPPA Compliance Manual: Training, audit and requirement checklist*. Retrieved March 17, 2010, from SearchSecurity.com: http://searchsecurity.techtarget.com.

U.S. Department of Health and Human Services. (2010). *Health Information Privacy*. Retrieved March 2, 2010, from HHS.gov: http://www.hhs.gov/ocr/privacy.

U.S. Department of Health and Human Services. (2010). *Health Information Privacy.* Retrieved March 30, 2010, from HHS.Gov: http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.hmtl.

United States Department of Labor. (2010). *Health Plans and Benefits*. Retrieved February 19, 2010, from United States Department of Labor: http://www.dol.gov/dol/topic/health-plans/protability.htm.

University of California. (2008). *PII & Information Security Training*. Retrieved March 3, 2010, from Berkley Lab: www.IBL.gov/cyber/training/pii/index.

University of Vermont. (2010). *HIPAA Identifiers*. Retrieved April 8, 2010, from University of Vermont College for Medicine: http://www.med.uvm.edu/research.

UTMB. (2002, April 10). *UTMB Office of Instituional Compliance.* Retrieved February 16, 2010, from Overview of HIPAA: http://www.utmb.edu/compliance.

Yahoo Answers. (2010, February 7). *Is this a HIPAA violation?* Retrieved March 30, 2010, from Yahoo Answers: http://answers.yahoo.com/question/index?qid20100207.

AMA. (2010). *Frequently asked questions about the HIPPA privacy*. Retrieved February 24, 2010, from AMA American Medical Association: http://www.ama-assn.org/ama/pub/physician-resources

businessballs.com. (2010). *businessballs.com*. Retrieved March 31, 2010, from presentation skills: http://www.businessballs.com/presentation.htm

Chicago Department of Public Health. (2005, April 20). *HIPPA 100 Training Manual.* Retrieved Febraury 16, 2010, from HIPPA Training Manual: http://www.uic.edu/nursing/forms/Clinical_Site_Requirements/CDPA/HIPPA

Dea MD, R., Cooper MD, T., & Cohen MD, S. (2003). *HIPPA: What's True, What Isn't*. Retrieved March 3, 2010, from The Permanente Journal: http://xnet.kp.org/permanentejournal/03/hippa.hmtl

Hackett, D. D., Schumacher, L., & Winget, R. (1995). *Train the Trainer.* Wichita Kansas: Wichita State Universtiy.

Health and Human Services. (1996, August 21). *Public Law Health Insurance Poertability and Accountability Act of 1996.* Retrieved March 21, 2010, from ASPE Health and Human Services: http:aspe.hhs.gov/admnsimp/p104191.htm

HIPPA Training.Net. (2010). *HIPPA Training and Compliance Solutions*. Retrieved March 15, 2010, from HIPPA TRAINING.NET: http://www.hippatraining.net/index.hmtl

HIPPA.ORG. (2003). *Unsure how to handle HIPPA?* Retrieved February 24, 2010, from HIPPA.ORG: www.hippa.org/

Noe, R. A. (2008). *Employee Training and Development.* New York: McGraw-Hill Irwin.

Privacy Rights Clearinghouse. (2010, January). *Medical Privacy in Electronic Age*. Retrieved March 25, 2010, from Privacy Rights Clearinghouse: http://www.privacyrights.org/fs/fs8-hippa.htm

SearchSecurity.com. (2009, April 13). *HIPPA Compliance Manual: Training, audit and requirement checklist*. Retrieved March 17, 2010, from SearchSecurity.com: http://searchsecurity.techtarget.com

U.S. Department of Health and Human Services. (2010). *Health Information Privacy*. Retrieved March 2, 2010, from HHS.gov: http://www.hhs.gov/ocr/privacy

United States Department of Labor. (2010). *Health Plans and Benefits*. Retrieved February 19, 2010, from United States Department of Labor: http://www.dol.gov/dol/topic/health-plans/protability.htm

University of California. (2008). *PII & Information Security Training*. Retrieved March 3, 2010, from Berkley Lab: www.IBL.gov/cyber/training/pii/index

Verespej, M. (2005, July 1). *HIPPA violation liability narrowed*. Retrieved February 19, 2010, from ALLBusiness: http:www.allbusiness.com/government/advocacy-consumer-protection.hmtl