HIPAA TRAINING HANDBOOK

An Introduction to the HIPAA Privacy Rule

Lexington-Fayette County Health Department

By Teresa L. Davis, Compliance/Privacy Officer

April 2003
(Revised July 2005)

Purpose of This Handbook

1. Provide an overview of the Health Insurance Portability and Accountability Act (HIPAA).
2. Inform you of the necessity to maintain privacy and security of patient information.
3. Alert you to the impact on your job activities.
4. Inform you of the consequences of non-compliance.
5. Explain the Compliance/Privacy Officer's role.
6. Provide a test to document your understanding of HIPAA.

Operational Process

Human Resources:

1. Issue the HIPAA Training Handbook to employee on the date of hire.
2. Notify the Compliance/Privacy Officer of the employee's name, supervisor, and hire date.

New Employee:

1. Read the handbook carefully.
2. Direct your questions to your supervisor or the Compliance/Privacy Officer (Teresa Davis at Extension 353)
3. Take test.
4. Submit completed test to your immediate supervisor within three (3) days.

Supervisor:

1. Review test.
2. Discuss test with employee ensuring that incorrect answers are corrected with explanations.
3. Sign test on page 19.
4. Send test to the Compliance/Privacy Officer.

Compliance/Privacy Officer:

1. Review test.
2. Send copy of test results to the new employee.
3. Send original test results to Human Resources.
4. Follow-up on any delays in return of test results with the employee's supervisor.

Human Resources:

1. Files test results in the training record.
2. Enter test completion in log.

What is HIPAA?

- The Health Insurance Portability and Accountability Act of 1996, or "HIPAA" for short.

- A Federal law which governs three areas:

  1. Insurance Portability - Ensures that individuals moving from one health plan to another will have continuity of coverage and will not be denied coverage under pre-existing condition clauses.

  2. Privacy and Security of Health Information - Requires physical, technical, and administrative safeguards be maintained.

  3. National Standards for Electronic Health Care Transactions - Identifies the identifiers, transactions, and code sets that must be used to transmit health information.

HIPAA Privacy Rule Major Goals:

- To establish appropriate safeguards to protect the confidentiality of health information in any form, whether oral, written, or Electronic.

- To give clients more control over uses and disclosures of their health information.

- Set boundaries for the use and disclosure of health records.

Who is Covered by the Privacy Rule?

- The Privacy Rule applies to the Lexington-Fayette County Health Department because it is a covered entity that electronically transmits health information for claims, benefit eligibility, referral authorizations, and other transactions.

The Privacy Rule's Impact on Public Health

The Privacy Rule recognizes the legitimate need for those who are responsible for ensuring the public's health and safety to have access to protected health information to conduct their mission. It provides for the continued functioning of the public health system.

The Privacy Rule expressly permits :

- PHI to be shared for specific public health purposes.
- Disclosures that are required by other laws that require disclosures for public health purposes.
- Pubic health authorities to receive reports for the purpose of preventing or controlling disease, injury, or disability. This includes:
    - Reporting of disease or injury
    - Reporting of vital events such as births or deaths
    - Conducting public health surveillance, investigations, or interventions
    - Reporting of child abuse and neglect
    - Monitoring of adverse outcomes to food, drugs, biological products, and medical devices

What is Confidential and Private?

Practically everything that has to do with **p**rotected **h**ealth **i**nformation - (PHI)!

What does PHI include?

Any information, including demographic information, collected from an individual, that …

(1) is created by a healthcare provider, health plan, employer, or a healthcare billing company.

(2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or for payment for the provision of healthcare.

(3) identifies the individual, or there is a reasonable basis to believe that the information can be used to identify the individual.

Straight from HIPAA

How is Patient Information Used?

Treatment: Provision, coordination, or management of healthcare and related services.

Operations:

- Quality Improvement (e.g.—Case management, program evaluations)
- Competency & Performance Reviews
- Conducting Training Programs (e.g.—Students in health care learn under supervision)
- Legal and Audit Services
- Business Planning and Development (e.g.— Compliance activities, some fund-raising, and marketing)
- Accreditation, Credentialing, Certification, and Licensing

Payment: Activities to obtain payment of claim referrals from one provider to another and to pay claims including:

- filing claims
- determining eligibility
- obtaining prior approval

What is "Use" vs. "Disclosure"?

Use	Disclosure
The sharing, utilization, examination, or analysis of PHI *within* the department or with business associates.	The release, transfer, provision of access to, or divulging in any other manner of PHI *outside* the department.

General Rule: Make reasonable efforts to limit the information to the **"minimum necessary"** in order to accomplish the intended purpose of the use, disclosure, or request. Follow all Department policies and procedures in your work area.

Let's Count the Ways…(1, 2, 3, 4…)

1. When you use it.
2. When you disclose it.
3. When you store it.
4. When you see it on your computer.
5. When it is lying on your desk.
6. When you share it with another healthcare provider.
7. When you are talking about it face to face.
8. When you talk about it over the phone.

Are you getting the picture??????

How May an Individual be Identified?

Here are some ways...

- Name
  - Birthdate
    - County or city
      - Zip code
        - Medical list
          - Telephone numbers
            - FAX numbers
              - E-mail address
            - Social Security number
          - Health Record number
        - Insurance cards
      - Account number
    - License plate number
  - Facial photographs
- Any other unique identifiers

In other words
NOT
just the health record.

Who is Authorized to See Information?

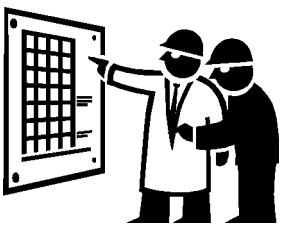
ONLY those who "**need to know"** to do their job, such as:

- Doctors, nurses, nutritionists, social workers, and other healthcare professionals and staff who need to assist and/or determine what care or services should be given to a client…

- **..and others, when necessary, as required by stricter laws:**

  - Public Health Purposes:
    - Birth or death records
    - Reportable disease or injury
    - Public Health surveillance, investigation, or intervention
    - The Food & Drug Administration (FDA)
    - Coroners & funeral directors
    - Report child/adult abuse

  - Other Examples:
    - Workers Compensation
    - Law enforcement officials
    - Others you can discuss with your supervisor



Ways to Protect Health Records..

1. Remember that loose reports and documentation regarding a patient should never be visible to the public or to those who do not need to know.

2. Health records should never be left unattended on counters or even in racks where they might pose a risk of inappropriate disclosure.

3. When disposing of patient information, shred it or dispose of it in an approved and secure manner. Do not simply toss it in the trash can under your desk.

4. Be mindful of what you leave showing on your computer screen. Use an automatic screen saver or close any program that contains PHI when leaving your desk.

5. Take reasonable precautions in whatever you do and wherever you are to protect the privacy and security of PHI.

6. Lock unattended files that contain PHI.

7. Use a dedicated FAX machine and copier.

8. Verify that a FAX number is correct before you push send and then *recheck* the number.

9. *Before* faxing information, ensure the intended person is on the receiving end.

10. Retrieve your incoming FAX immediately.

11. Don't leave copies unattended on the copier.

Patients' Rights

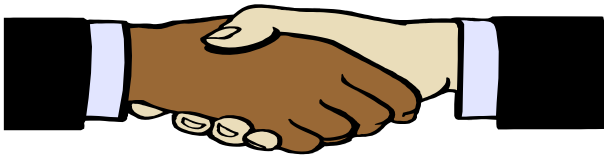
HIPAA says a patient has a right to:

- **"Notice of Privacy Practices"** which contains how their PHI may be used or disclosed
- Right to request restrictions
- Have access to their PHI
- Inspect, copy, amend
- Accounting of disclosures except for treatment, payment, and health care operations (Starting 4-14-03)
- List exceptions to the rule, such as, more stringent laws that we follow (e.g. Public Health Laws)
- Be informed on how to file a complaint with the Compliance/ Privacy Officer and/or the Office of Civil Rights (OCR)

We must attempt to obtain proof of our notification effort with a

- **signature from all patients on an "Acknowledgement Receipt."**

Privacy and Security Go Hand-In-Hand!



Security must be provided to protect the *privacy* of patient information so that PHI does not land in the wrong hands. Security measures are those that safeguard the physical storage, maintenance, and access to PHI.

Your Part:

- Keep discussions about patient care private to reduce the likelihood that those who do not need to know will not overhear.
- Shred paper records or place them in a locked shred-it bin.
- Do not leave your computer logged on to protected information while you are not at your workstation.
- Turn your computer screen away from the view of the public or people passing by.
- Keep all PHI maintained in the work area covered from the public.
- If you find records unattended, return them to Health Records.

Health Department's Part:

- Security guard after hours
- Sign-in and out with badge
- Computer passwords and unique identifiers required
- Background checks
- Audits and monitoring
- Computer maintenance (e.g. virus checking)
- Building Security

What is the Role of the Compliance/ Privacy Officer?

- Advocates and protects patient privacy by serving as a key contact for patients, staff, and contractors.
- Handles complaints: receive, document, track, investigate, and take action on all complaints concerning privacy policies and procedures.
- Manages patient requests regarding their PHI rights.
- Maintains current knowledge of applicable federal and state privacy laws to ensure adaptation and compliance.
- Assists all program personnel with compliance issues.
- Your Compliance/Privacy Officer is Teresa Davis, J.D., Human Resources, Extension 353.

Your Role...

- Report any privacy violations to your supervisor. However, you may report your concerns to the Compliance/Privacy Officer without fear of retaliation.

It's right. It's the law.

- Curb human nature: curiosity and sharing inappropriately.
- Be sensitive: respect patient rights to the privacy of his/her health information.
- Know the Department's policies and procedures.
- Understand how and when to disclose information.

Why You Should Take HIPAA Seriously

It is important to know that there are penalties for failure to meet the requirements of the Privacy Rule or inappropriately disclosing or receiving PHI. Penalties can be either criminal or civil and can result in monetary fines, or imprisonment up to 10 years depending on the severity. Penalties become more severe when information is obtained with the intent to sell or transfer it, or use for commercial, personal gain, or malicious harm. Both institutions & individuals can be held liable for breaches in privacy.

What does a "breach" mean?

A breach is defined as ***"any unauthorized or unnecessary use or disclosure of confidential information"*** due to carelessness, curiosity, concern, and particularly willingly or maliciously.

Result = An employee may receive an oral/written warning, suspension, or even termination.

Doing Your Part

- Only access confidential information if you need it to do your job.
- Protect your computer passwords.
- Understand the law and the Department's policies and procedures.
- Treat patients' PHI the way you would want your PHI treated.
- Read *HIPAApoints* posted monthly in the Healthy Tymes newsletter.
- Discuss your questions and issues with your supervisor.
- Keep confidential information that you learn while employed at the Health Department **H E R E**.

Remember: HIPAA is not about refusing to share information but sharing information as needed and protecting PHI while you work.

HIPAA TEST

(Directions: Circle the correct answer.)

1. A patient's confidential information may include his or her:

a. Social Security number
b. Address
c. Age
d. Name
e. All of the above

2. Which of the following phrases should you keep in mind when determining whether you should have access to patient information?

a. Any information out in the open is public record.
b. Disregard all patient information.
c. Need to know.
d. All of the above.

3. The criminal penalties for improperly disclosing PHI can be either monetary fines and /or up to 10 years imprisonment depending on the severity of the breach.

True False

4. If you see a neighbor in the health department, is it all right to mention to someone that you saw the neighbor at the health department?

Yes No

Go to the next page ►

5. Under what circumstances are you free to repeat to others PHI that you hear on the job?

a. After you no longer work at the Department.
b. After a patient dies.
c. Only if you believe that the patient would not mind.
d. When authorized for your job duties.

6. If you suspect someone is in violation of the Department's privacy policy, you should:

a. confront the individual involved and train them on the policies.
b. watch the individual involved until you have gathered solid evidence against him or her.
c. Report your suspicions to your supervisor or to the Compliance/Privacy Officer.
d. Do nothing at all.

7. Which of the following are some common safeguards designed to protect PHI?

a. Locks on health records files
b. Passwords to access the computer system
c. Rules that prohibit employees from looking at records unless they have a need to know.
d. All of the above.

8. Only employees who need access to patient records have to worry about protecting patient privacy and confidentiality.

True False

Go to the next page ►

9. The Notice of Privacy Practices explains the ways the Department will use patient information and tells patients about their rights regarding the information.

True False

10. Any employee, volunteer, or physician who violates the Department's privacy policies is subject to punishment up to and including being fired.

True False

11. HIPAA has provisions that allow healthcare workers to report suspected cases of child abuse to the police.

True False

12. PHI that must be protected by employees includes a patient's past, present and future physical or mental health condition, but not billing information.

True False

13. What kind of PHI is protected by HIPAAs privacy rule?

a. Spoken
b. Written
c. Electronic
d. All of the above

Go to the next p a g e ►

HIPAA Training Handbook Test

I, _____ have read and understand
([PRINT NAME)
the HIPAA Training Handbook, and have answered all the test questions to the best of my ability.

Signature _____ Date _____
([NEW EMPLOYEE)
Supervisor's Name _____ Division _____
(PRINT)
Signature _____ Date _____
(SUPERVISOR)

Remove test portion from the HIPAA Training Handbook and return to your supervisor no later than three (3) days after your first day of work.

Date assigned by Human Resources _____.

You will be notified of your test results *within* 30 calendar days by the Compliance/Privacy Officer who will also clarify any missed answers (if any). Your original test results will be placed in your personnel record and you will receive a copy.

Score: ____ Signed _____Date: _____
Compliance/Privacy Officer