HIPAA: PRIVACY COMPLIANCE

COASTAL HEALTH + TRAIN

HIP000-HBK-ENG-0005

www.coastal.com

10-2005

HIPAA: PRIVACY COMPLIANCE

This employee handbook is one of a series of fully illustrated employee handbooks, informative posters, broadcast-quality video training programs, interactive CD-ROM and Web-based courses produced by Coastal HealthTrain, a division of Coastal Training Technologies Corporation. Each product is the result of painstaking analysis, design, development and production by the instructional designers and technical specialists on our staff.

Our catalog is constantly being revised and expanded, so we would appreciate any comments on current titles or suggestions for future ones. For further information on any Coastal product, or to receive a free HealthTrain catalog, call Coastal Training Technologies Corp. (Virginia Beach, VA) at 1-800-729-4325 or send a FAX to 757-498-3657. Visit us on the Web at www.coastal.com.

This handbook is for educational purposes only, and is designed to be used in conjunction with a qualified trainer. Nothing herein is to be regarded as indicating approval or disapproval of any specific practice or product.

CONTENTS

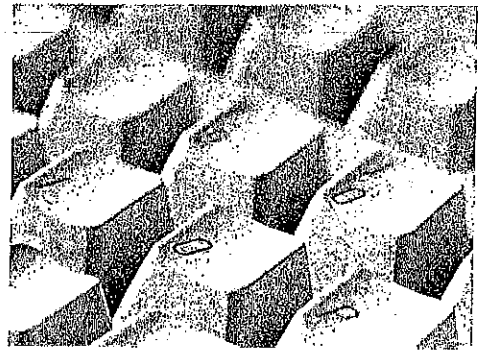
HIPAA: PRIVACY COMPLIANCE

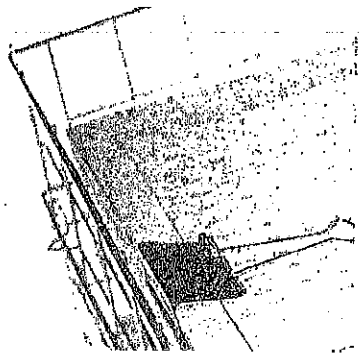
The HIPAA Privacy Rule — finalized on August 14, 2002 — ensures that personal medical information you share with doctors, hospitals and others who provide and pay for healthcare is protected. It is part of the Health Insurance Portability and Accountability Act (HIPAA) enacted by Congress.

Basically, the Privacy Rule does the following:

- Imposes new restrictions on the use and disclosure of personal health information
- Gives patients greater access to their medical records
- Gives patients greater protection of their medical records.

You can make sure you protect personal patient data by learning the basics of the final HIPAA Privacy Rule outlined in this handbook.



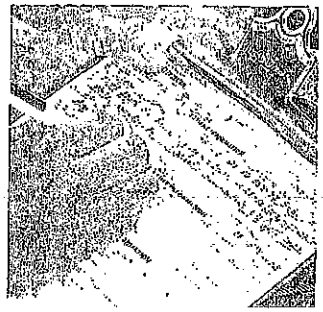


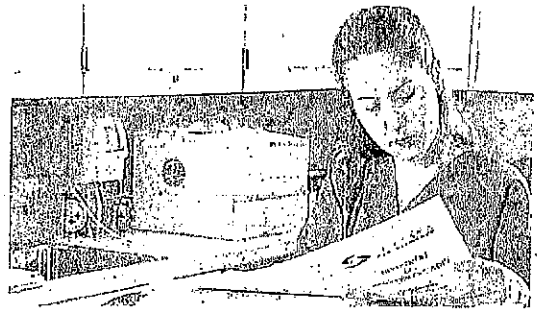
WHO IS COVERED BY THE HIPAA PRIVACY RULE?

You're covered by the HIPAA Privacy Rule — and termed a covered entity — if you are a:

- Healthcare provider
- Health plan
- Healthcare clearinghouse

HIPAA also indirectly affects business associates who have access to patient records.





WHAT IS PROTECTED HEALTH INFORMATION?

When a patient gives personal health information to a covered entity, that information becomes Protected Health Information – or PHI.

PHI includes any information – oral, recorded, on paper, or sent electronically – about a person's physical or mental health, services rendered or payment for those services, and that includes personal information connecting the patient to the records.

Examples of information that might connect personal health information to the individual patient include:

- The individual's name or address
- Social security or other identification numbers
- Physician's personal notes
- Billing information.

WHAT ARE THE RULES FOR THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION?

HIPAA's Privacy Rule is all about the use and disclosure of Protected Health Information or PHI. With few exceptions, PHI can't be used or disclosed by anyone unless it is permitted or required by the Privacy Rule.

PHI is used when:

- Shared
- Examined
- Applied
- Analyzed.

PHI is disclosed when:

- Released
- Transferred
- In any way made accessible to anyone outside the covered entity.

You are permitted to use or disclose PHI:

- For treatment, payment, and healthcare operations
- With authorization or agreement from the individual patient
- For disclosure to the individual patient
- For incidental uses such as physicians talking to patients in a semi-private room.

You are required to release PHI for use and disclosure:

- When requested or authorized by the individual – although some exceptions apply
- When required by the Department of Health and Human Services (HHS) for compliance or investigation.

WHEN IS AUTHORIZATION REQUIRED?

The final ruling makes consent for routine healthcare optional. But you are required to get a signed authorization from the patient if you use or disclose his or her Protected Health Information for purposes other than:

- Treatment
- Payment
- Healthcare operations.

Generally, authorization is required to use PHI:

- For use or disclosure of psychotherapy notes
- For research purposes, unless a documented waiver is obtained from the Institutional Review Board (IRB) or a privacy board
- For use and disclosure to third parties for marketing activities such as promoting services or selling lists of patients.

However, covered entities may communicate freely with patients about treatment options and health-related information.

WHAT IS INCLUDED IN AN AUTHORIZATION FORM?

Each authorization form only covers the use/disclosure outlined in that form. The form must contain:

- A description of the PHI to be used/disclosed, in clear language
- Who will use/disclose PHI, and for what purpose
- Whether or not it will result in financial gain for the covered entity
- The patient's right to revoke the authorization
- A signature of the patient whose records are used/disclosed, and a date of signing
- An expiration date.

WHEN IS AUTHORIZATION NOT REQUIRED?

PHI can be used/disclosed without authorization, but with patient agreement, for the following reasons:

- To maintain a facility's patient directory
- To inform family members or other identified persons involved in the patient's care, or notify them on patient location, condition or death
- To inform appropriate agencies during disaster relief efforts.

Other permitted uses/disclosures that do not require patient authorization or agreement include:

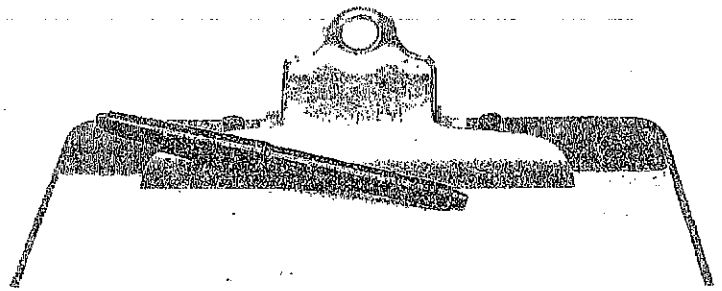
- Public health activities related to disease prevention or control
- To report victims of abuse, neglect, or domestic violence
- Health oversight activities such as audits, legal investigations, licensure or for certain law enforcement purposes or government functions
- For coroners, medical examiners, funeral directors or tissue/organ donations
- To avert a serious threat to health and safety.

WHAT IS MINIMUM NECESSARY?

In general, use/disclosure of PHI is limited to the minimum amount of health information necessary to get the job done right. That means:

- Covered entities must develop policies and practices to make sure the least amount of health information is shared
- Employees must be identified who regularly access PHI along with the types of PHI needed and the conditions for access.

The Minimum Necessary requirement does not apply to use/disclosure of medical records for treatment, since healthcare providers need the entire record to provide quality care. But it does apply in all other circumstances.



WHAT IS THE NOTICE OF PRIVACY PRACTICES?

Patients have the right to adequate notice concerning the use/disclosure of their PHI on the first date of service delivery, or as soon as possible after an emergency. And new notices must be issued when your facility's privacy practices change.

The Notice of Privacy Practices must:

- Contain patient's rights and the covered entities' legal duties
- Be made available to patients in print
- Be displayed at the site of service, and posted on a web site whenever appropriate.

Once a patient has received notice of his or her rights, covered entities must make an effort to get written acknowledgement of receipt of notice from the patient, or document reasons why it was not obtained. And copies must be kept of all notices and acknowledgements.

WHAT ARE PATIENT PRIVACY RIGHTS?

The Privacy Rule grants patients new rights over their PHI. It's your job to make sure they can exercise their rights, including the following:

- Receive Notice of Privacy Practices at time of first delivery of service
- Request restricted use and disclosure, although the covered entity is not required to agree
- Have PHI communicated to them by alternate means and at alternate locations to protect confidentiality
- Inspect and amend PHI, and obtain copies, with some exceptions
- Request a history of disclosures for six years prior to the request, except for disclosures made for treatment, payment, healthcare operations or with prior authorization
- Contact designated persons regarding any privacy concern or breach of privacy within the facility or at HHS.

WHAT ABOUT THE PRIVACY RIGHTS OF MINORS?

In general, parents have the right to access and control the PHI of their minor children — except when state law overrides parental control. Examples include:

- HIV testing of minors without parental permission
- Cases of abuse
- When parents have agreed to give up control over their minor child.

WHAT MUST ADMINISTRATION DO TO COMPLY?

- Allow patients to see and have copies made of requested PHI.
- Designate a full- or part-time privacy official responsible for implementing the programs.
- Designate a contact person or office responsible for receiving complaints.
- Develop a Notice of Privacy Practices document.
- Develop policies and safeguards to protect PHI and limit incidental use or disclosure.
- Institute employee-training programs, so everyone knows about the privacy policies and procedures for safeguarding PHI.
- Institute a complaints process, and file and resolve formal complaints.
- Make sure all business associate agreements comply with the Privacy Rule.

WHAT HAPPENS TO THOSE WHO DON'T COMPLY?

If you violate the Privacy Rule, HIPAA set civil and criminal penalties including:

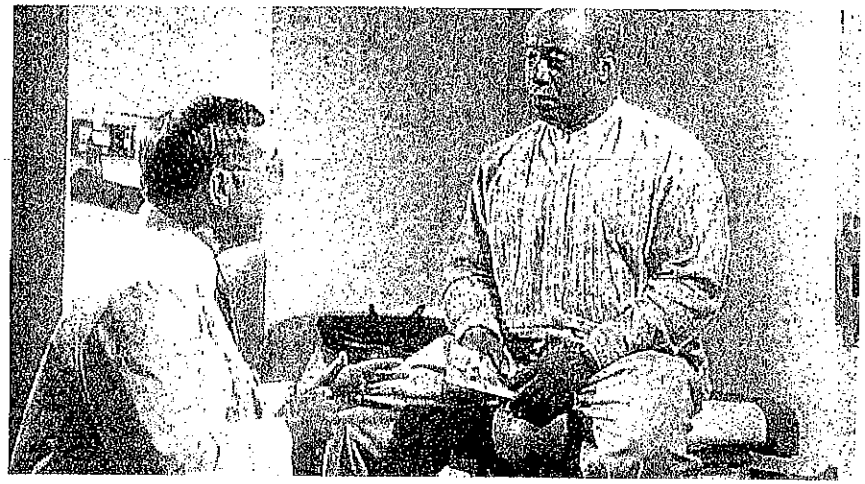
- A $100 civil penalty up to a maximum of $25,000 per year for each standard violated
- A criminal penalty for knowingly disclosing PHI — a penalty that may escalate to a maximum of $250,000 for conspicuously bad offenses.

But if you unknowingly make a mistake, remember: the Department of Health and Human Services is mandated to give you and your organization advice and technical assistance — and help you work out problems.

WHAT CAN YOU DO TO PROTECT PATIENTS' PRIVACY AND CONFIDENTIALITY?

HIPAA protects our fundamental right to privacy and confidentiality. And that means HIPAA's Privacy Rule is everyone's business – from the CEO to the healthcare professional to the maintenance staff. To do your part:

- Make sure you fully understand your facility's privacy practices.
- Protect your patients' personal health information.
- Encourage others to do the same.



QUIZ

1.	True	False	The HIPAA Privacy Rule protects a patient's fundamental right to privacy and confidentiality.
2.	True	False	You are called a covered entity if you are a healthcare provider, health plan, or healthcare clearinghouse who transmits health information in electronic form.
3.	True	False	Protected Health Information is anything that connects a patient to his or her health information.
4.	True	False	PHI includes all health information that is used/disclosed – except PHI in oral form.
5.	True	False	PHI is disclosed when it is shared, examined, applied or analyzed.
6.	True	False	PHI is used when it is released, transferred, or allowed to be accessed or divulged outside the covered entity.
7.	True	False	You are permitted to use/disclose PHI for treatment, payment and healthcare operations.
8.	True	False	You are required to use/disclose PHI when authorized or requested by the individual patient.
9.	True	False	Using PHI for purposes not specified by the rule requires covered entities to get patient authorization.
10.	True	False	Authorization must be obtained for any use/disclosure of PHI for marketing purposes.
11.	True	False	An authorization must contain an expiration date.
12.	True	False	After signing an authorization, the patient can decide to revoke it.

QUIZ continued

13. True False — You must obtain patient agreement to use/disclose PHI for public health activities related to disease prevention.

14. True False — You can use/disclose PHI without patient agreement to report victims of abuse, neglect or domestic violence.

15. True False — In general, disclosure of PHI must be limited to the least amount needed to get the job done right.

16. True False — The Notice of Privacy Practices gives patients notice about the use/disclosure of their PHI, as well as their rights in general.

17. True False — The Privacy Rule gives patients the right to request a history of routine disclosures.

18. True False — The Privacy Rule gives patients the right to take action if their privacy is violated.

19. True False — If you need help understanding the rules, the Department of Health and Human Services is required to give you assistance.

20. True False — To protect patient confidentiality, learn about your facility's patient privacy rights — and encourage others to do the same.

ACKNOWLEDGEMENT OF TRAINING

I have read and understand the training handbook, *HIPAA: Privacy Compliance.* I have also completed and passed the comprehensive quiz at the conclusion of this handbook.

Employee's Signature _____ Date _____

Trainer's Name _____ Date _____

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

All at Home
HEALTH CARE

_QUIZ (HIPPA)

1. The HIPAA Privacy Rule protects a patient's fundamental right to privacy and confidentiality. True ____ False____

2. You are called a covered entity if you are a healthcare provider, health plan, or healthcare clearinghouse who transmits health information in electronic form. True____ False____

3. Protected Health Information is anything that connects a patient to his or her health information. True ____ False____

4. PHI includes all health information that is used/disclosed —except PHI in oral form. True____ False ____

5. PHI is disclosed when it is shared, examined, applied or analyzed.

   True____ False ____

6. PHI is used when it is released, transferred or allowed to be accessed or divulged outside the covered entity.

   True____ False____

7. You are permitted to use/disclose PHI for treatment, payment and healthcare operations. rue□

8. You are required to use/disclose PHI when authorized or requested by the individual patient. False

9. Using PHI for purposes not specified by the rule requires covered entities to get patient authorization. b4rue C] False

10. Authorization must bp obtained for any use/disclosure of PHI for marketing purposes. False

11. An authorization must contain an expiration date. True False

12. After signing an authorization, the patient can decide to revoke it. True False

13. You must obtain patient agreement to use/disclose PHI for public health activities related to disease prevention. True

14. You can use/disclose PHI without patient agreement to report victims of abuse, neglect or domestic violence. True False

15. In general, disclosure of PH must be limited to the least amount needed to get the job done right. True False

16. The Notice of Privacy Practices gives patients notice about the use/disclosure of their PHI, s well as their rights in general. True False

17. The Privacy Rule gives patients the right to request a history of routine disclosures. True

18. The Privacy Rule gives patients the right to take action if their privacy is violated. U True False

19. If you need help understanding the rules, the Department of Health and Human Services is required to give your assistance. True C] False

20. To protect patient confidentiality, learn rights — and encourage others to do the same.

Acknowledgement of Training

I've read and understand the training handbook, HIPAA: Privacy Compliance. I've also completed and passed the comprehensive quiz at the conclusion of this handbook.