HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT

Privacy Awareness
April 5, 2006

Presented by Anne Adams
Chief Compliance Officer
Emory Healthcare and Emory Medical Care Foundation
Chief Privacy Officer, Emory Healthcare
Privacy
The right of an individual to be left alone, including freedom from intrusion into one’s private affairs and the right to maintain control over certain personal information.

Confidentiality
The responsibility for limiting disclosure of private matters including the responsibility to use, disclose, or release such information with the knowledge and consent of the individual.

Security
The means to control access and protect information from accidental or intentional disclosure to unauthorized personnel and from alteration, destruction or loss.
Standards for Privacy of Individually Identifiable Health Information (IIHI)

- To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information.

- To improve the quality of health care in the United States by restoring the trust in the health care systems among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care.

- To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems and individual organizations and individuals.
Also Provides for:

- Patient control over their health information.
- Sets boundaries on the use and release of health records.
- Accountability - civil and criminal penalties.
- Public responsibility - protect public health.
- Establishes a federal floor of safeguards to protect privacy of patient information.
Who & What?

• The Health Insurance Portability and Accountability Act contains standards to protect the privacy of individually identifiable health information.

• Protected Health Information is any information that identifies the past, present or future physical or mental health of an individual, and includes all communication media - written, verbal and electronic.

• Extends to all individually identifiable health information in the hands of covered entities (health care provider).

• Health care provider - a provider of medical services. . . and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
Verbal Communications

- Elevators
- Hallways
- Cafeteria
- Public Areas
- Avoid using patient’s name
- Reasonably safeguard to minimize inadvertent disclosure
- Post signs
- Educate
• Uses and Disclosures, Treatment, Payment, Health Care Operations.

• “Minimum necessary” - a disclosure of protected health information, even where authorized by the regulations, must be limited to the “minimum necessary” to accomplish the purpose for which it is made. (Does not apply to disclosures to or request by a health care provider for treatment purposes).

• Special requirements for use of protected health information for research purposes, requiring approval by an Institutional Review Board or a privacy board. IRB may approve waiver of authorization based on specific criteria.

• Facility Directories - Name, Location, Status (religious affiliation to Chaplains).
- Public Health Activities / Agency
- Law Enforcement
- Use of Patient Information for Fundraising - Opt-Out
- Use of Patient Information for Marketing - Opt-In
- Confidential Communication
- Right to Request Restrictions
- Psychotherapy Notes - Authorization
- Verification of Identity
- Safeguards
- Non-retaliation
Authorization and

The Notice of Privacy Practices

Notice of Privacy Practice - what is it? Document given to patients beginning April 14, 2003 on their first date of receiving service that explains the covered entity’s privacy practices and use and disclosure of health information.

Authorization - must be written in specific terms - specify the particular information to be used or disclosed and who will receive the information; contains an expiration date; must be obtained for use or disclosure of psychotherapy notes; for use and disclosure of protected health information created for research.
<table>
<thead>
<tr>
<th>Identifiers of Protected Health Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Address</td>
</tr>
<tr>
<td>Zip</td>
</tr>
<tr>
<td>Names of relatives</td>
</tr>
<tr>
<td>Name of employer</td>
</tr>
<tr>
<td>DOB</td>
</tr>
<tr>
<td>Telephone number</td>
</tr>
<tr>
<td>Fax number</td>
</tr>
<tr>
<td>E-mail address</td>
</tr>
<tr>
<td>Finger or voice prints</td>
</tr>
<tr>
<td>Photographic images</td>
</tr>
<tr>
<td>SSN</td>
</tr>
<tr>
<td>Medical record number</td>
</tr>
<tr>
<td>Health plan beneficiary number</td>
</tr>
<tr>
<td>Account number</td>
</tr>
<tr>
<td>Certificate/license number</td>
</tr>
<tr>
<td>Vehicle or other device serial number</td>
</tr>
<tr>
<td>IP address</td>
</tr>
<tr>
<td>Any other unique identifier, character, code</td>
</tr>
<tr>
<td>Any other identifying information that could reasonably identify the patient.</td>
</tr>
</tbody>
</table>
De-Identification of Protected Health Information and Limited Data Sets

De-Identification

Health Information that does not identify an individual and there is no reasonable basis to believe that the information can identify an individual is not individually identifiable health information.
Health information is considered de-identified if:

• The risk is very small that the information could be used to identify an individual.

• Removal of all of the identifiers of the individual - safe harbor.

• EHC may use codes or other similar means of marking records so they may be later re-identified.
HIPAA requires that covered entities receive an authorization for use and disclosure of PHI for research purposes prior to the covered entity disclosing the information except in limited circumstances.

**Waiver of Authorization**

- Approval by IRB or Privacy Board; Date of approval.
- **Exceptions:** The researcher would need to represent that the use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposed preparatory to research, no protected health information is to be removed from covered entity by the researcher in the course of the review and the protected health information for which use or access is sought is necessary for the research purposes and information recorded is de-identified.
Exceptions continued:

Research on decedent's information is permitted without authorization as long as:

• Researcher represents that the use or disclosure sought is solely for research on the protected health information of decedents.

• Researcher must provide documentation of the death of the individuals if requested.

• Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes. (In this case, access should be given to the decedents records).
Patient Rights

- Right to receive a notice describing the covered entity’s privacy practices.
- Inform patients how to file complaints, either with the covered entity or DHHS.
- Identify a contact person who can provide additional information.
- Right to access, inspect, and copy protected health information that is used, in whole or in part, to make decisions about them.
- Right to request amendment of protected health information.
Patient Rights

• Right to receive an accounting of disclosures made by a covered entity for purposes other than treatment, payment, and health care operations made within six years prior to the request.

• The accounting must be provided within 60 days after receipt of the request.

• Right to request restrictions on the use and disclosure of their protected health information. Not required to agree to these requests, but if they do, they must abide by them, except in emergencies.

• Patients may ask health care providers and plans to communicate health information to them by “alternative means” or at “alternative locations”.
Administrative Procedures

Covered entities must have policies, procedures and systems in place to protect health information and individual rights. Requirements include:

• designation of a privacy officer
• office to register complaints
• privacy training for employees
• safeguards to prevent intentional or accidental misuse of protected health information
• sanctions for employee violations
Civil and Criminal Penalties for Violation

Enforcement of the privacy regulations has been delegated to the DHHS Office of Civil Rights.

Improper use or disclosure of PHI can result in the following fines and/or imprisonment, as set forth under HIPAA:

• Civil monetary penalties for HIPAA privacy violations are $100 per incident, up to $25,000 per person, per year, per transaction standard violated - this is enforced by CMS.

• A person who knowingly violates HIPAA and obtains PHI or discloses PHI to another person may be fined up to $50,000 and imprisoned up to one year, or both.
Civil and Criminal Penalties for Violation

- If the offense is committed under false pretenses, the fine may be up to $100,000 and imprisonment up to five years.
- If the offense is committed with the intent to sell, transfer, or use IIHI for commercial advantage, personal gain, or malicious harm, the fine may be up to $250,000 and imprisonment up to 10 years.
Privacy Tips for Providers and Others for Safeguarding Patient Information

• Make sure that you follow the policies and procedures.

• Make sure that patient information is destroyed either through shredding or placing in a locked collection box. Get paper shredder for your area.

• Conduct a walk about in your area to identify where you may have privacy and security concerns.

• One of the easiest things is to make sure your computer screen is not visible to anyone but you.

• When you get up from your desk, do not leave any patient information sitting out in plain view, and make sure you log-off of your computer.
• Don’t provide anyone with your computer log-in or password.

• Don't talk about patients in public areas such as elevators, buses, cafeterias, or restaurants.

• Take extra precautions if your work area is accessible by the public.

• Keep patient information and records behind your work area.

• If you are transporting patient information make sure the identifiable information isn't showing.

• At the end of the day, make sure you have properly shut down your computer and LOCK all your file drawers that contain patient information.
WEB RESOURCES

http://www.hipaadvisory.com

http://aspe.hhs.gov/admnsimp/

http://hippo.findlaw.com/hipaa.html

http://www.healthprivacy.org/