The following program is presented by
Penny C. Wofford
of
Edwards, Ballard, Bishop,
Sturm, Clark and Keim, P.A.

Ms. Wofford is a frequent speaker on topics of employement law, family leave, discrimination, and employee benefits. Ms. Wofford assists entities in the development of HIPAA Compliance Programs.

Developing a Practical Medical Privacy Program

Sponsored by:
American Furniture Manufacturers Association

February 6, 2003
Hickory, North Carolina

Presented by:
PENNY C. WOFFORD, ESQ.

Edwards, Ballard, Clark, Barrett and Carlson, P.A.
Post Office Box 1708
Winston-Salem, NC 27102-1708
336-750-0707

Edwards, Ballard, Bishop, Sturm, Clark and Keim, P.A.
Post Office Box 5398
Spartanburg, SC 29304
864-542-8612

Edwards, Ballard, Bishop, Sturm, Clark and Keim, P.A.
One Town Square Blvd., Ste. 341
Asheville, NC 28803
828-687-4071

www.edwardsballard.com

Requirements of the Privacy Rule

Protected Health Information

Individually identifiable health information

In *any* form

- Electronic
- Written
- Oral

That is created or received by a covered entity

DE-IDENTIFIED INFORMATION

Health information that does not identify an individaul and with respect to which there is no reasonable basis to believe that information can be used to identify any individual is not subject to the Privacy Rule.

DE-IDENTIFIED INFORMATION

(cont'd)

Information is de-identified when the following 18 identifiers are removed:

1. Names
2. All geographic subdivisions smaller than a state *(i.e., street address, city, county, zip code)*
3. All elements of dates (except year) directly related to an individual *(i.e. birth date, admission date, discharge date)*
4. Telephone numbers

DE-IDENTIFIED INFORMATION

(cont'd)

5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate / license numbers
12. Vehicle identifiers and serial numbers

DE-IDENTIFIED INFORMATION

(cont'd)

14. Web Universal Resource Locator (URL)
15. Internet protocol (IP) address number
16. Biometric identifiers, including finger or voice prints
17. Full face photographic images and comparable images
18. Any other unique identifying number, characteristic or code

Limited Data Set

Responds to circumstances where more information than is included in de-identified information is needed to accomplish certain purposes.

Limited Data Set

1. Research
2. Public health
3. Health care operations

Limited Data Set

A limited Data Set is protected health information so other restrictions in Privacy Rule apply.

Designated Record Set

A group of records maintained by or for a covered entity that is:

1. Medical and billing records
2. Enrollment, payment, claims adjudication, and case or management records systems; or
3. Records used by the covered entity to make decisions about the individual

MINIMUM NECESSARY RULE

For routine disclosures, only the *minimum amount* of information necessary to accomplish the intended purpose can be disclosed.

MINIMUM NECESSARY RULE

(cont'd)

The minimum necessary standard does *not* apply to:

- Disclosures to or requests by health care providers for treatment purposes.
- Dislcosures to the individual.
- Uses or disclosures made pursuant to an individuals authorization.
- Uses or disclosures required for compliance with HIPAA.
- Disclosures to HHS for enforcement purposes.
- Uses or disclosures required by other law.

MINIMUM NECESSARY RULE

(cont'd)

The Rule allows a covered entity to rely on the judgment of the requesting party regarding the minimum amount of information needed. Such reliance is permitted when the request is made by:

- A public official or agency who states that the information requested is the minimum amount necessary.
- A nother covered entity.
- A professionl workforce member or business associate who states that the information requested is the minimum amount necessary.
- A researcher with appropriate documentation.

Personal Representatives

A person authorized (under state or other applicable law) to act on behalf of the individual in making health care related decisions.

Personal Representatives

Under the Privacy Rule, a personal representative stands in the shoes of the individual and has the ability to act for the individual and exercise the individual's rights.

PERSONAL REPRESENTATIVES

Who must be recognized as a personal representative:

INDIVIDUAL	PERSONAL REPRESENTATIVE
Adult or Emancipated Minor	Health Care Power of Attorney Court appointed legal guardian General Power of Atty
Unemancipated Minor	Parent or Guardian
Deceased	Executor of estate Next of kin or Family member

Non-Routine Disclosures
(Non-TPO)

Those disclosures relating to:

Marketing

Employment decisions; **OR**

Non-health purposes.

MARKETING

A covered entity must have an authorization to use protected health information for marketing. Marketing does *not* include:

- Disease management, health prrevention, preventive care and wellness programs;
- Descriptions of health care provider networks; and
- Health plan communications about health-related products or value-added services.

BUSINESS ASSOCIATES

Any person or organization who on behalf of a covered entity performs or assists in the performance of a function or activity involving the use or disclosure of protected health information.

BUSINESS ASSOCIATES

Covered entities may disclose protected health information to business associates **ONLY** to help the covered entity carry out health care or health plan functions - *not* for the business associate's independent use or purposes.

BUSINESS ASSOCIATES

(cont'd)

Situations in which a Business Associate contract is *not* required:

- Disclosures by a covered entity to a health care provider for treatment of the individual
- With persons or organizations *(i.e. janitorial services)* whose services do not involve use or disclosure of protected health information.
- With persons or organizations that act merely as a conduit for protected ehalth information *(i.e. US Postal Service, private couriers, etc.)*.
- When a covered entity purchases a health plan product or other insurance *(i.e. reinsurance)*.

BUSINESS ASSOCIATES

The Final Modifications to the Privacy Rule:

- Give covered entities up to an additional year to change existing contracts (except small health plans)
- Provides a model business associate contract provision

BUSINESS ASSOCIATES

(cont'd)

Responsibilities during the contract transition period:

1. Make information available to HHS, including information held by business associate;
2. Fulfill an individual's rights to access and amend protected health information, including information held by covered entity; and
3. Mitigate, to the extent practicable, any harmful effect that is known regarding impermissible use or disclosure of protected health information by a business associate.

SANCTIONS

A covered entity must have and apply appropriate sanctions against members of its workforce who *fail* to comply with the entity's policies and procedures or the HIPAA privacy rule.

Requirements for Privacy Forms

PRIVACY NOTICE

Covered entities are requireed to provide individuals with a privacy notice *except* a group health plan which:

- Is fully insured or an HMO; and
- Does not create or receive protected health information other than summary health information or enrollment and participation information

PRIVACY NOTICE

(cont'd)

Three critical elements for compliance:

1. Content and delivery of the notice;
2. Individual's acknowledgment of receipt of the notice; and
3. Covered entity's policy and procedures related to the notice.

CONTENT OF THE PRIVACY NOTICE

SAMPLE PRIVACY NOTICE

[Organization] Privacy Notice

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

[Organization] uses health information about you for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care that you receive. Your health information is contained in a medical records that is the physical property of [Organization].

How [Organization] May Use or Disclose Your Health Information

For Treatment. [Organization] may use your health information to provide you with medical treatment or services. For example, information obtained by a health care provider, such as a physician, nurse, or other person providing health services to you, will record information in your record that is related to your treatment. This information is necessary for health care providers to determine what treatment you should receive. Health care providers will also record actions taken by them in the course of your treatment and note how you respond to the actions.

For Payment. [Organization] may use and disclose your health information to others for purposes of received payment for treatment and services that you receive. For example, a bill may be sent to you or a third-party payor, such as an insurance company or health plan. The information on the bill may contain information that identifies you, your diagnosis, and treatment or supplies used in the course of treatment.

For Health Care Operations. [Organization] may use and disclose health information about you for

DISTRIBUTION OF THE PRIVACY NOTICE

Health Plans must provide a Privacy Notice to:

the named insured of a policy that provides coverage;

to individuals covered by the plan on April 14, 2003 (for small health plans on April 14, 2004);

to new enrollees at the time of enrollment; and

to all individuals covered by the plan within 60 days of a material revision to the plan.

DISTRIBUTION OF THE PRIVACY NOTICE

(cont'd)

Health Plans

At least once every 3 years, the plan must notify individuals covered by the plan of the availability of the notice and how to obtain it.

DISTRIBUTION OF THE PRIVACY NOTICE

(cont'd)

A covered entity must prominently post and make available its notice on any website it maintains that provides information about its customer services or benefits.

DISTRIBUTION OF THE PRIVACY NOTICE

(cont'd)

Health Care Providers and Company Nurses

Health care providers with a direct treatment relationship must:

- Deliver the notice no later than the first service delivery after April 14, 2003
- In an emergency treatment situation, the notice must be delivered as soon as reasonably practical following the emergency

DISTRIBUTION OF THE PRIVACY NOTICE

(cont'd)

Health Care Providers and Company Nurses

The notice must be available at the physical site of service delivery and must be posted in a prominent location

The notice must be available upon request on or after the effective date of any revision

DISTRIBUTION OF THE PRIVACY NOTICE

(cont'd)

Health Care Providers and Company Nurses

Must make a good faith effort to obtain a written acknowledgment from the individual regarding the receipt of the notice.

AUTHORIZATIONS

SAMPLE AUTHORIZATION FORM

Authorization for the Use and Disclosure of Individually Identifiable Health Information

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that the information I authorize a person or entity to receive may be re-disclosed and no longer protected by federal privacy regulations.

1. Persons/organizations within the covered entity authorized to use or make disclosure of the information:

_____

_____

2. Persons/organizations authorized to receive the information:

_____

_____

3. Specific description of information that may be used/disclosed:

_____

_____

4. This authorization permits the use and disclosure of health care information for marketing purposes as described below. NO_____ YES_____

5. If the anser to 4 is YES, [Organization name] WILL_____ WILL NOT _____ receive remuneration from a third party for the use of this health care information.

6. The information will be used/disclosed for the following purposes [*all* purposes must be listed and described]:

Purpose 1

_____

_____

Purpose 2

_____

_____

7. I understand that this authorization is voluntary and that I may refuse to sign this authorization. Unless allowed by law, my refusal to sign will not affect my ability to obtain treatment; receive payment; or eligibility for benefits.

8. I understand that I may revoke this authorization at any time by notifying the person/organization providing the information in writing. However, the revocation will not be valid if [organization] has taken action in reliance on this authorization; or

9. This authorization expires on [upon] _____ [INSERT APPLICABLE DATE OR EVENT]

_____	_____
Signature of Individual	Date
_____	_____
Printed name of patient or patient's representative	Relationship to patient or authority to act for the patient

[*If the above signature is that of a patient's representative, [Organization] must complete the following.]* [Name of organization] has verified the identity of [patient's representatives name] by [describe means of verification, e.g., driver's license] and that in his/her capacity of [description of authority to act, e.g., husband, wife, etc.], he/she is authorized to act on behalf of the patient.

Administrative Requirements

DOCUMENTATION REQUIREMENTS

1. Maintain policies and procedures;
2. Maintain communications that are required to be in writing; and
3. Maintain a written or electronic records of all actions, activities or designations that are required to be documented.

Documentation Requirements

(Communications required to be in writing)

- Health plan documents
- All signed consents and authorizations
- The privacy notice and acknowledgment form
- Business Association contracts

Documentation Requirements

(Actions required to be documented)

- Education and training
- Privacy staff appointments
- Individual's requests for information
- Complaints and their resolution

PRIVACY TRAINING

Covered entities must train all employees who work with the health plan on the entity's privacy policies and procedures.

DOCUMENTATION REQUIREMENTS

(cont'd)

Education and Training

- The nature of the training
- The name of the training session
- The date and location
- The amount of training provided
- A copy of training materials used
- Attendance or participation records
- Background qualifications of trainer
- Pre and post test results
- Students' evaluations of the training
- Any results of training

DOCUMENTATION REQUIREMENTS

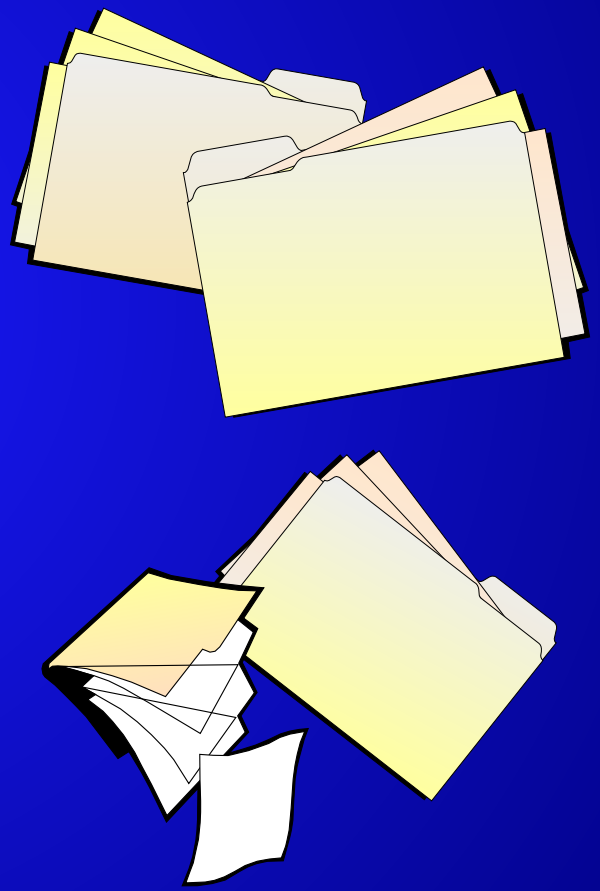
(cont'd)

Privacy Staff Appointments

- Privacy officer
- Contact person for information and complaints
- Persons to receive and process access requests
- Persons to receive and process requests for amendment of PHI
- Persons to receive and process requests for accounting for PHI disclosures
- Persons to approve release of de-identified information

Individual's Rights to Information

- Right to copies.
- Right to amend to records.
- Right to receive an accounting of disclosures.
- Right to request restrictions.
- Right to file a complaint.



DOCUMENTATION REQUIREMENTS

(cont'd)

Individual Requests for Information

- Requests for Access of PHI
  - *Extension of time to respond to an access request*
  - *Denial of access request*
- Requests for Restrictions and Agreement to Same
- Request for Amendment of records
  - *Extenstion of time to respond to an amendment request*
  - *Decision on amendment request*

DOCUMENTATION REQUIREMENTS

(cont'd)

Requests for Accounting of Disclosures

Extension of time to respond to an accounting

Copies of all accountings provided

Complaints, Investigations and Sanctions Imposed

RECORD RETENTION PERIOD

Covered entities are required to maintain documentation for 6 years from the date of its creation or the date when it was last in effect, which ever is later.

Safeguarding Protected Health Informatiohn

PHYSICAL SECURITY

- Limit access to offices or areas where PHI is maintained.
- Supervise unauthorized personnel and vistors.
- Lock doors and file cabinets
- Manage the distribution of keys or entry codes.

PROTECTING PRINTED INFORMATION

- Limit opening of incoming mail.
- Clean desk.
- Transmit information in envelopes.
- Use a secure fax machine
- Shred documents containing PHI for discarding.

PROTECTING ELECTRONIC INFORMATION

Password protect electronic data.

Breaking diskette

Cut up CDs

DISCLAIMER

The information herein should not be construed as legal advice. Regulations, guidance and legal opinions continue to change with HIPAA as with any new law. This presentation is meant for informational content only. Neither the presenter, Edwards, Ballard, Bishop, Sturm, Clark and Keim, P.A., nor AFMA make any warranty of any kind concerning this information. You should seek the advice of your attorney for additional or specific information.