

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 employment 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 5, 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](http://www.edwardsballard.com)

# Final Rule on Medical Privacy

- Mandated by the Health Insurance Portability and Accountability Act (**HIPAA**)
- Enforced by the Office for Civil Rights (OCR) in the U.S. Department of Health and Human Services (HHS)



# Background

- Released on December 28, 2000, but stayed until April 14, 2001 by Executive Order of President Bush.
- Guidance issued by OCR on July 6, 2001.
- Proposed modifications issued on March 21, 2002.
- Final modifications issued on August 9, 2002.

# Background

State and federal laws which provide stronger privacy protections will continue to apply over and above the federal Rule on Medical Privacy

# Covered Entities

- Health Care Clearinghouses
- Health Care Providers - *who transmit any health information in electronic form*
- Health Plans - *whether insured or self-funded which have:*
  - ▶ 50 or more participants; **OR**
  - ▶ are administered by an entity other than the employer that established and maintains the plan

# Health Plans

- Health
- Dental
- Vision
- Medical Flexible  
Spending Account

# Entities specifically NOT covered

- Employers
- PlanSponsors
- Life, Disability, and Workers' Compensation Insurers
- BusinessAssociates



# Compliance Dates

- April 14, 2003
- April 14, 2004  
*(small health plans - annual receipts of \$5 million or less)*

# Small Health Plan Annual Receipts

## Fully Insured

Use the total premiums paid  
for health benefits.

## Self Insured

Use the total amount paid  
for health care claims.

# Employment Records

The final modifications to the rule excludes employment records from the definition of protected health information. A covered entity must use a functional test in determining whether a record is an employment record.

# Permitted Uses And Disclosures

- To the individual involved;
  - For routine disclosures for health purposes with or without the individual's consent;
- OR**
- With the individual's *authorization*, to make non-routine disclosures.

# Protected Health Information

- Individually identifiable health information
- In *any* form
  - ▶ Electronic
  - ▶ Written
  - ▶ Oral
- That is created or received by a covered entity

# Routine Disclosures

Those disclosures necessary to carry out:

- Health care **T**reatment;
- Health care **P**ayment; *OR*
- Health care **O**perations.

# TPO

Healthcare Treatment - provision, coordination or management of healthcare and related services by one or more healthcare providers.

Healthcare Payment - activities undertaken by a health plan or provider to obtain reimbursement or premiums for the provision of healthcare including coordination of benefits, eligibility or coverage determinations, billing, collections, and utilization reviews.

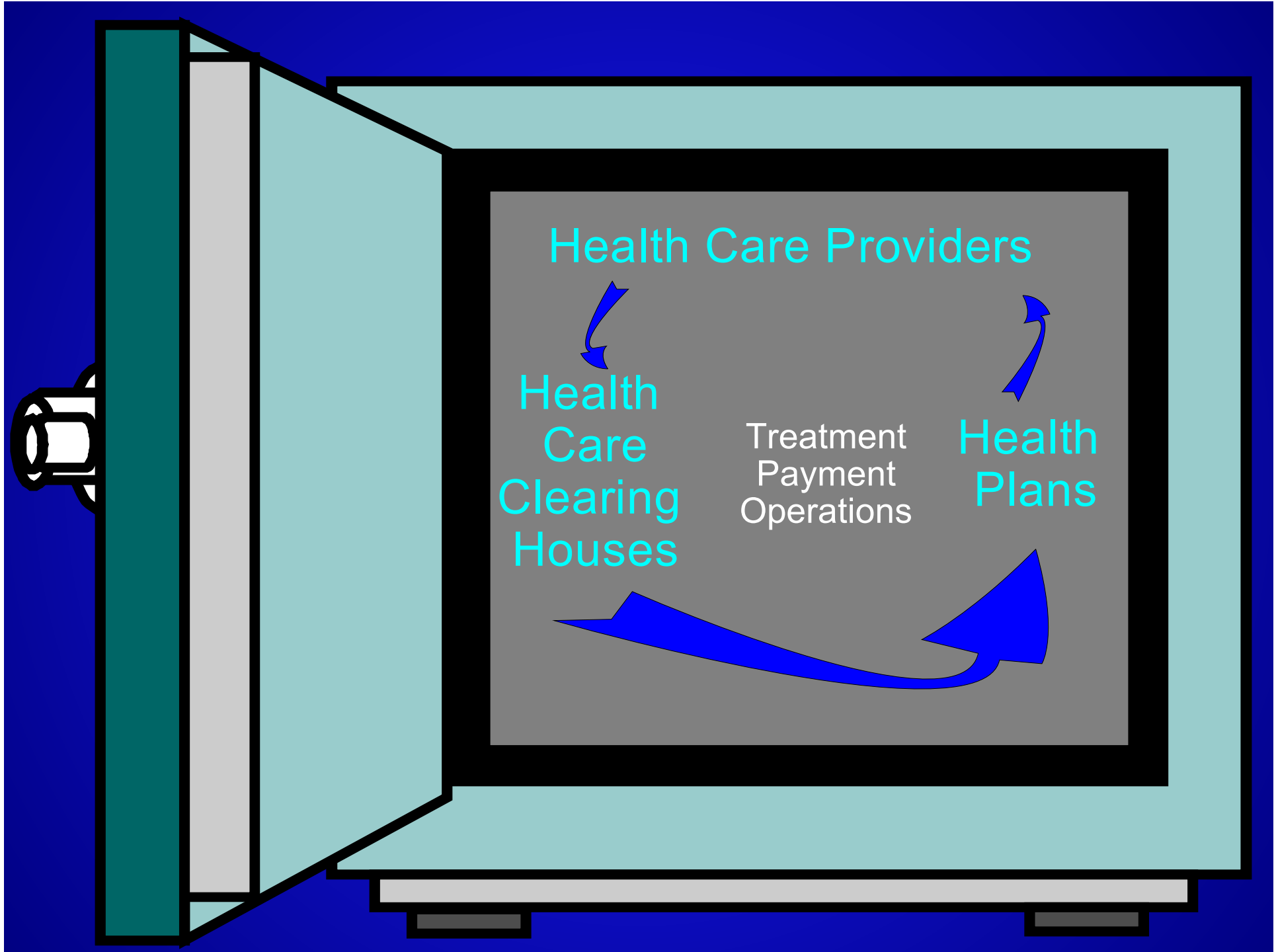
# TPO

Healthcare Operations - services or activities necessary to carry out a covered entities treatment or payment such as certification or licensing requirements, evaluation of provider performance, underwriting or premium rating, auditing claims and deciding claims appeals.



# Routine Disclosures (TPO)

Permissible with or without the individual's consent under the final modifications to the rule.



Health Care Providers

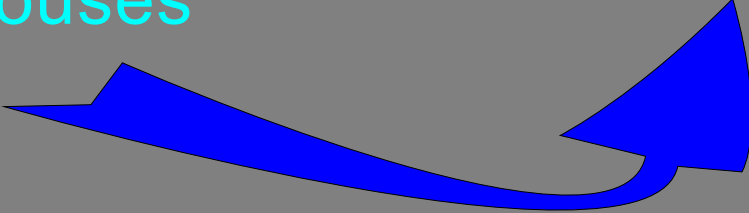


Health  
Care  
Clearing  
Houses

Treatment  
Payment  
Operations



Health  
Plans



# Minimum Necessity Rule

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

# Non-Routine Disclosures (Non-TPO)

Those disclosures relating to:

- Marketing
- Employment decisions; **OR**
- Non-health purposes.

# Non-Routine Disclosures

**MUST GET A  
WRITTEN  
AUTHORIZATION**

# Authorization For Disclosures

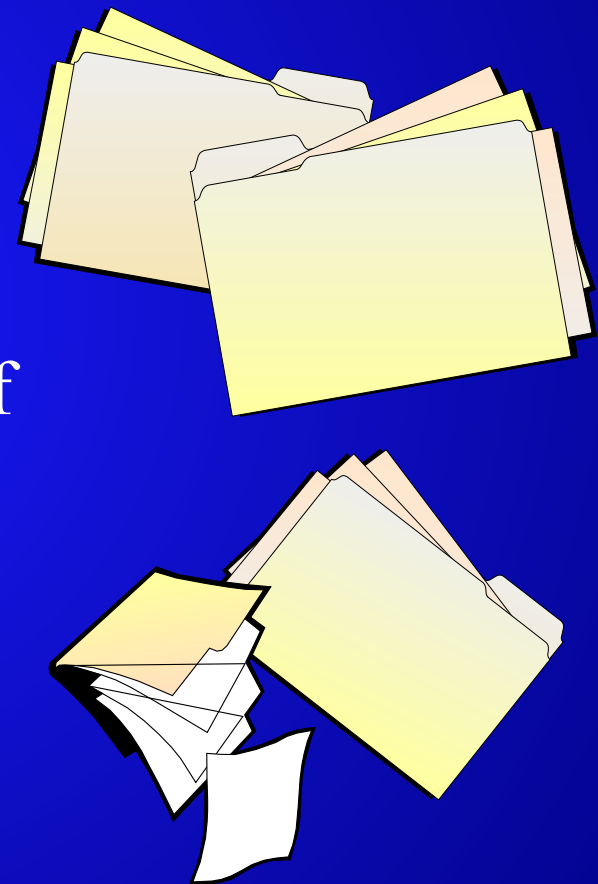
Cannot condition enrollment in a health plan upon an individual's providing an authorization.

# Incidental Disclosures

The final modifications to the rule permit certain incidental disclosures that occur as a by-product of an otherwise permitted disclosure. However, incidental disclosures are permitted only to the extent that a covered entity has applied reasonable and appropriate safeguards and implemented the minimum necessary standard.

# 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.





# Right to Copies

An individual has the right to inspect and obtain a copy of his/her protected health information maintained by a covered entity.

- A covered entity must provide access or copies within 30 days of receipt of a request (60 days if records are maintained off-site).

# Right to Copies

(Con't)

- A covered entity may impose reasonable fees including the cost of copying (including supplies and labor) and postage (if the copies are mailed). The fee cannot include costs associated with searching or retrieving the information.
- The rule does not require covered entities to document oral communications that is used for TPO.

# Right to Amend Records

An individual has the right to request amendment of protected health information maintained by a covered entity.

- A covered entity must act on a request for amendment within 60 days of the request.
- A covered entity may deny the request but must provide the individual with a notice explaining the denial and the individual's right to submit a statement of disagreement.

# Right to Receive an Accounting

An individual has the right to receive an accounting of disclosures of protected health information made by a covered entity for the 6 years prior to the request. The accounting must include the date of each disclosure, name and address of entity who received the information and a brief description of the information disclosed.

- Disclosures for **TPO** are excepted from the accounting requirement.
- A covered entity must act on an individual's request for an accounting within 60 days of receipt of the request.

# Right to Request Restrictions

An individual has a right to restrict uses and disclosures of his/her protected health information. A covered entity can deny the request but if it agrees, it must follow the individual's restriction. A covered entity must accommodate reasonable requests to receive communications relating to protected health information by alternative means.

# Right to File a Complaint

An individual has the right to file a complaint with a covered entity regarding the entity's use or disclosure of his/her protected health information. An individual may also file complaints with OCR.

# Business Associates

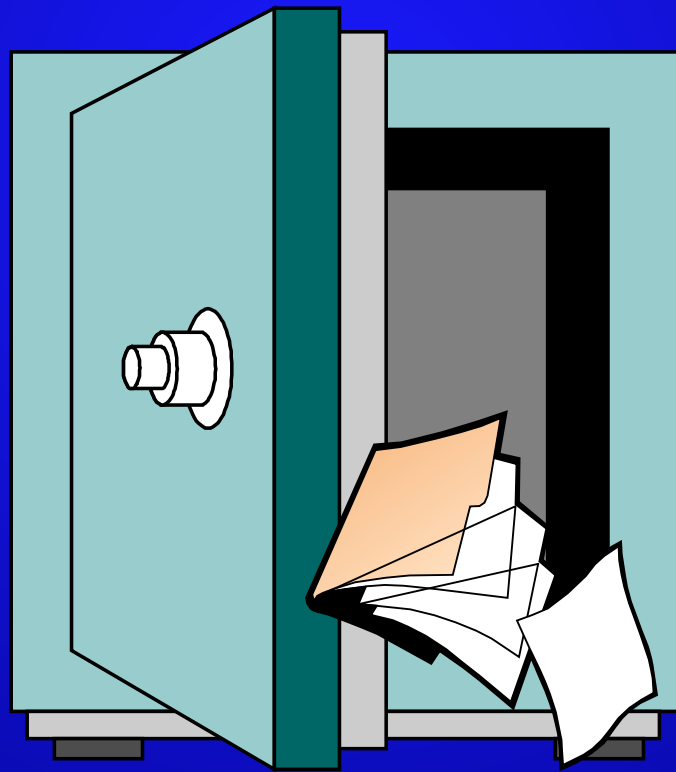
Includes anyone (or any entity) who provides services to the covered entity, including:

- Legal;
- Actuarial;
- Accounting;
- Accreditation;
- Financial Services;
- Consulting; or
- Administrative.



# Business Associates

Business Associates must agree, through contract, to safeguard protected health information.





# Business Associates

A covered entity is not required to monitor business associates.

However, if a covered entity discovers that a business associate has violated the contract, it must act to end the violation and if unsuccessful, terminate the contract with the business associate.

# Business Associates

At the time the contract is terminated, Business Associates must return or destroy all protected information, if feasible.

# 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

## 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

# Penalties

- Civil

- ▶ Up to \$25,000, per incident

- Criminal

- ▶ Up to \$50,000 fine and 1 year in prison
- ▶ Up to \$100,000 fine and 5 years in prison (obtaining information under false pretenses)
- ▶ Up to \$250,000 fine and 10 years in prison (obtaining or disclosing information for commercial or personal advantage or malicious harm)



# Complaints

The final rule does not provide a private right of action to individuals. However, individuals may file a written complaint with OCR. The complaint must be filed within 180 days when the complainant should have known that the act occurred.

# Plan Document Provisions

A health plan may disclose summary health information to allow the plan sponsor to obtain bids or to modify, amend or terminate a plan. If the plan sponsor wishes to obtain additional information the plan document must contain privacy information.

# Summary Health Information

Information that summarizes  
claims history, claims expenses  
or types of claims experienced by  
plan participants.



# Plan Document Provisions

The Plan must **state** that the sponsor will:

- Not disclose protected information to any other person;
- Not use information for employment decisions or in connection with any other plan;
- Allow individuals access to their information, consider requests for amendments, and provide an accounting upon request;
- Ensure that its business associates agree to similar restrictions;
- Describe which employees will have access to information and restrict use of information to the administrative functions; and
- Provide a mechanism for resolving noncompliance with its privacy policy.

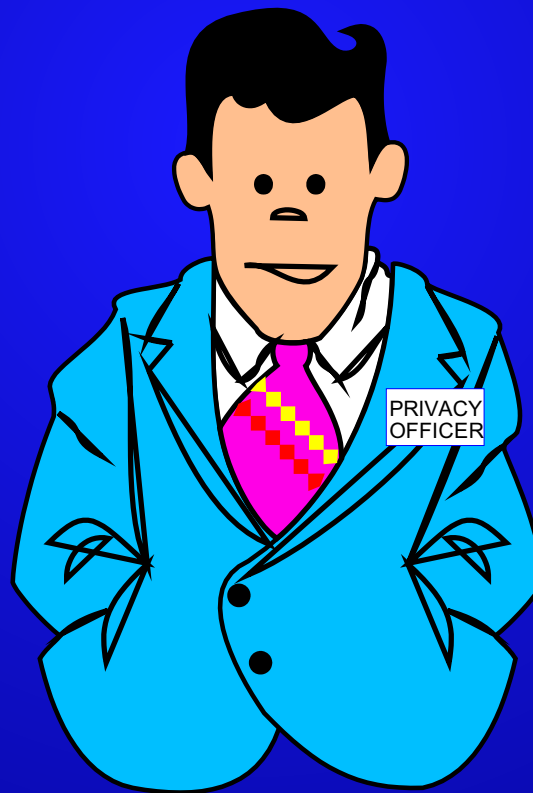
# Administrative Requirements

- Designate privacy officer.
- Develop privacy policies and procedures.
- Train employees to understand and comply with policies and procedures.
- Give individuals a health privacy notice.



# PRIVACY OFFICER

Covered entities must appoint a  
privacy officer.



# PRIVACY POLICIES AND PROCEDURES

Covered entities must have policies and procedures that reasonably limit access to and use of protected health information.

# PRIVACY POLICIES AND PROCEDURES

- Identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties;
- The categories and types of protected health information needed; and
- The conditions upon which such access is allowed.

# PRIVACY POLICIES AND PROCEDURES

The policies and procedures of a smaller health care provider may be more limited than that of a large health care provider such as a hospital.

# PRIVACY POLICIES AND PROCEDURES

The complaint procedure should require a written complaint and specify a person or office responsible for receiving such complaints.

# PRIVACY TRAINING

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



# PRIVACY NOTICE, CONSENTS, AND AUTHORIZATIONS

Health plans must develop a privacy notice and authorization forms that meet each of the specific requirements of the regulations.

# Privacy Notice

Covered entities must give individuals a written or electronic notice of the:

- Intended uses or disclosures of protected health information;
- An individual's right to protect such information;
- Duty of the covered entity to comply with privacy standards;
- An individual's right to file a complaint; and
- The name, title, and phone number of a contact person for complaints.

# Consent For Disclosures



***Can be general and without a limit on duration.***

But must:

1. Be written in plain language;
2. State that information will be used for treatment, payment, and operations;
3. Refer to privacy notice;
4. State that the individual has a right to revoke consent; and
5. Be signed and dated.

# Authorization For Disclosures

**Must be specific and of limited duration.**

**Must state:**

- 1 The information to be used/disclosed;**
- 2 The name of the covered entity;**
- 3 The name of the receiver of information;**
- 4 The right of the individual to revoke;**
- 5 The expiration date or event;**
- 6 That the information may be redisclosed by the receiver; and**
- 7 Be signed and dated.**

# Business Associates

## Contract must:

- Include the permitted uses of the protected information;
- Restrict the business associate from other uses or disclosures;
- Require the business associate to report any non permitted uses or disclosures; and
- Ensure that any agents or subcontractors to whom the business associate provides protected information agree to hold the information confidential.

# Implementation Plan

- 1.** Appoint a privacy officer and provide education on the Final Rule.
- 2.** Develop a plan with time frames.
- 3.** Analyze how health information flows and what types of disclosures are made within your organization.
- 4.** Close the gaps.

5. Review current forms and policies and revise to comply with HIPAA.
6. Develop a training plan for employees who received or use protected health information.
7. Inventory contractual relationships with business associates.
8. Audit and monitor procedures periodically.

[www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa)



# 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.