

NAF Health Benefits Program HIPAA Privacy Rules Training

PRIVACY IS OUR RESPONSIBILITY



2012

Agenda

- HIPAA Privacy Rules Background
- Penalties for Non Compliance
- Terminology and Definitions
- Protected Health Information
- Use and Disclosure of Information
- Rights of Employees
- Privacy Officer
- Complaints
- Security
- Compliance Strategy
- FAQs
- References for More Information



Introduction

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted by Congress with four mandates
- This training is focused on the HIPAA Privacy Rules which falls under one of those mandates, the Administrative Simplification Standard

Background

- Prior to the HIPAA Privacy Rule, your personal information could be used by hospitals, pharmaceutical companies, and brokers for marketing purposes
- Employers who had access to your private health information could use the information for retaliatory actions in employment
- Employees do not want employers and co-workers to know their various medical condition(s)

What are Retaliatory Actions in Employment?

- Hiring – discrimination due to potential expense to the plan
- Promotions/RIFs – medical condition plays a factor
- Terminations – due to medical conditions/treatments such as:
 - HIV
 - Psychiatric disorders
 - Drug addiction treatment programs

What does the Privacy Rule Do?

- Gives individuals greater access to their own medical records and medical information in personnel files
- Protects health information from being used unreasonably by imposing restrictions on the use and disclosure of personal health information
- Provides individuals with greater protection of their medical information

Who is covered by the Privacy Rules

- Covered entities include:

Health plans, health care providers, and health care clearing houses including:

- DoD NAF HBP (self insured health plan)
 - HMO
- All NAF authorized employees, those designated by the Privacy Official, who have access to protected health information

HIPAA Privacy Rules Compliance Date

- Starting April 14, 2003 the NAF HBP will comply with the HIPAA Privacy Rules law and regulations



Penalties for non Compliance

- The HHS Office of Civil Rights enforces the final privacy rule. There is no private right to a lawsuit contained within the privacy rules; individuals may file complaints with the Secretary of Health and Human Services.
- Failure to comply with the HIPAA Privacy Rules can result in a civil penalty of up to \$100 per incident and up to \$25,000 per person, per year, per standard.
- Criminal penalties will apply if a person knowingly discloses PHI and/or misuses a unique health identifier. Knowingly disclosing information can incur up to \$50,000 in fines and one year in prison. Obtaining information under false pretenses can result up to \$100,000 in fines and five years in prison.
- Gathering information with the intent to sell, transfer or use for commercial advantage results in up to \$250,000 in fines and up to 10 years in prison.

Sanctions for non Compliance

- The NAF HBP has procedures for disciplining authorized employees who abuse an individual's Protected Health Information
- Examples:
 - Retraining
 - Immediate Job Counseling
 - Documenting in Performance Appraisals
 - Reduction of Job Duties
 - Progressive Discipline Procedures

Employer and Health Plan Responsibilities

- Remember difference between health plan and employer
- Two separate entities
- Employer wears two hats
 - Health plan sponsor – governed by HIPAA
 - Employer – not governed by HIPAA

Excluded from HIPAA Privacy Rules

- Benefits **excluded** from the HIPAA Privacy Rules are:
 - Accident-only coverage
 - Disability Insurance
 - Worker's compensation
 - Liability Insurance
 - Life Insurance
 - Leave and Sick Programs
 - Information gathered for OSHA regulations
(Occupational Health and Safety Administration)

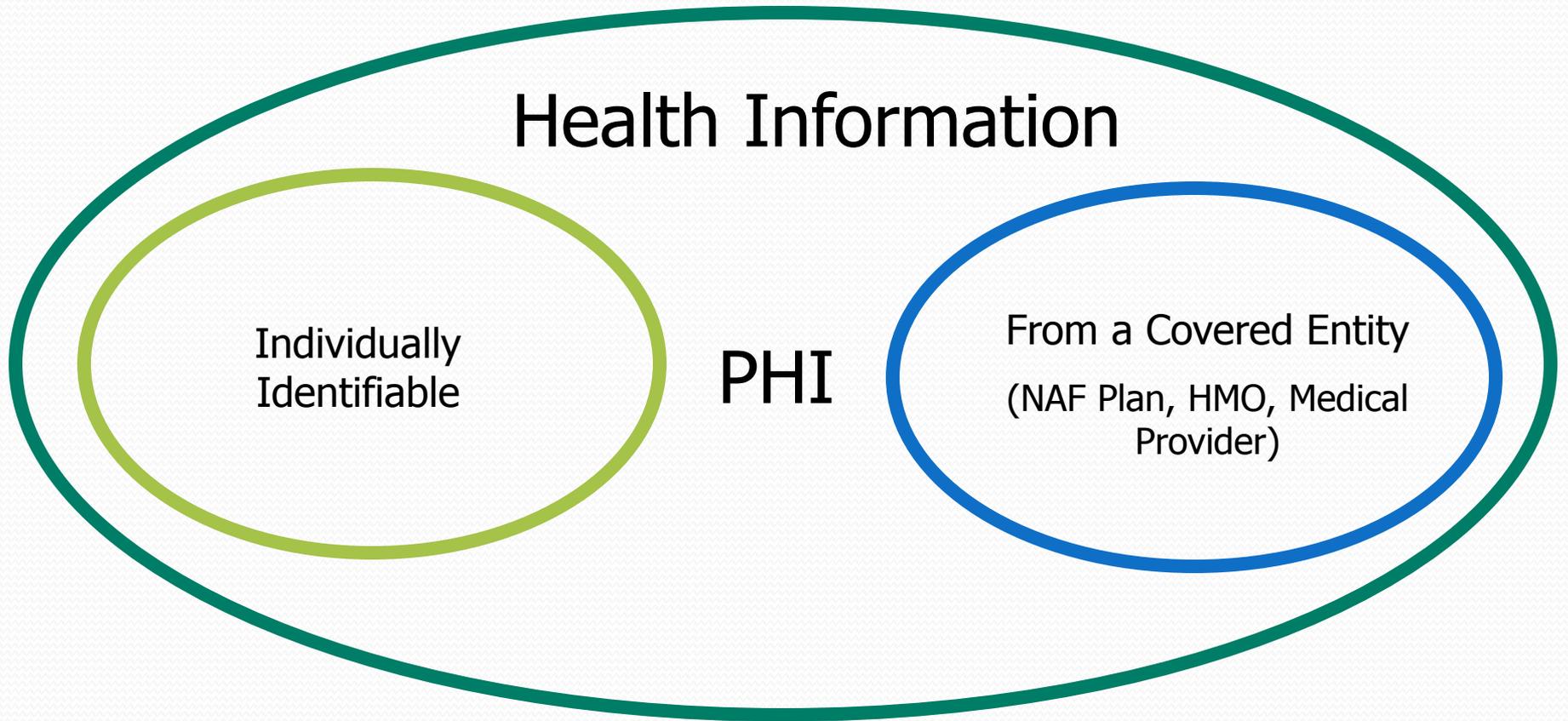
Frequently used Terms

- Authorized employee – those employees, designated by the NAF Privacy Official, who may have access to protected health information for their job duties
- PHI – Protected Health Information
- TPO – Treatment, Payment, or Health Care Operation
- De-Identified Information- PHI is considered de-identified if the unique identifier is removed and there is no reasonable basis to believe that the information may identify an individual
- Minimum Necessary Standard – a standard that when using PHI use the minimum PHI necessary in accomplishing the task.

What is Considered Protected Health Information (PHI)?

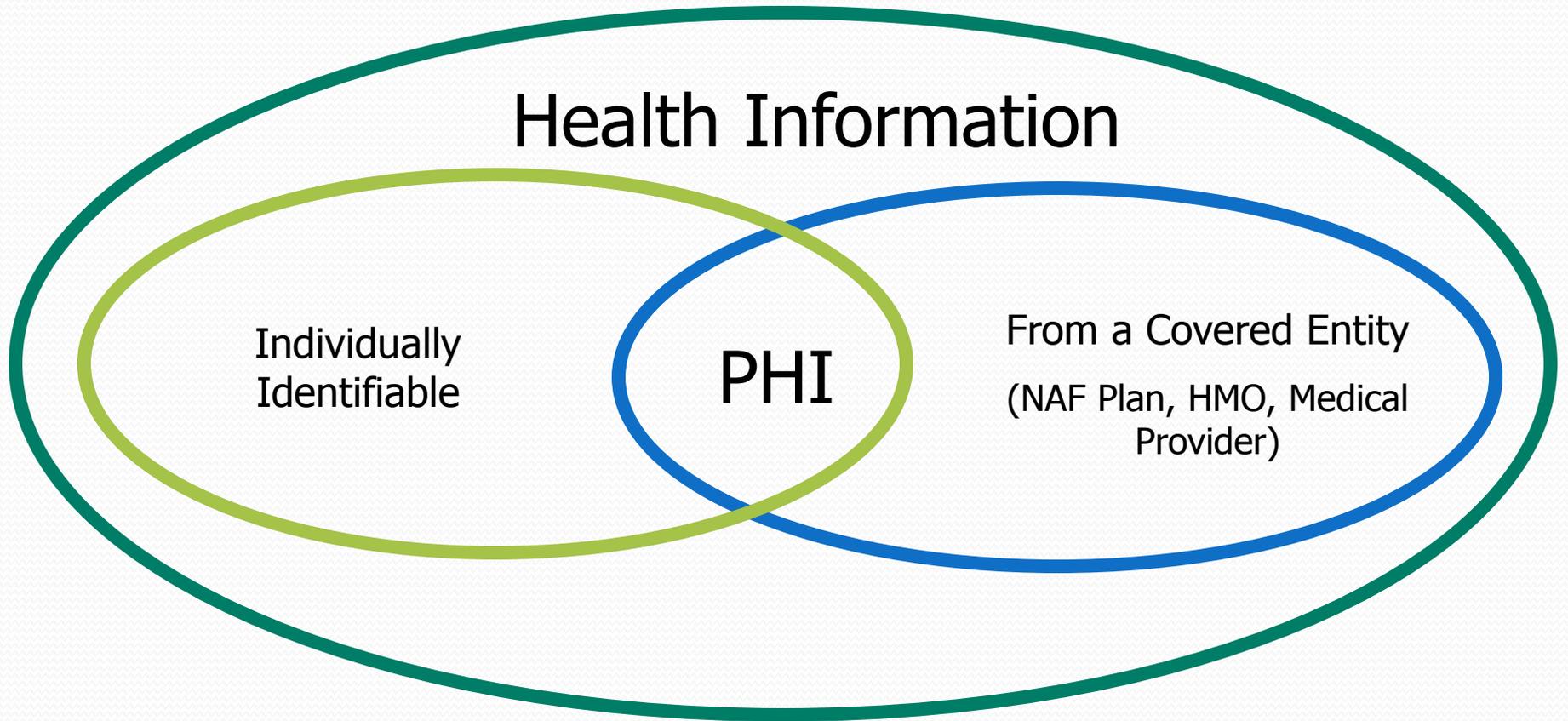
- The HIPAA Privacy Regulations govern the use and disclosure of a member's "protected health information" (PHI)
- For information to be PHI, it must:
 - Relate to the past, present, and future physical or mental health condition, the provision of health care, or the payment for health care
 - Identify, or could reasonably be used to identify, the individual
- The Privacy Regulations cover PHI that is transmitted or maintained in any form or medium (e.g., electronic, paper, fax, voice mail and oral communications)

PHI is a Subset of All Health Information



It is **NOT** PHI when identifiers are separate from health information.

PHI is a Subset of All Health Information



It **IS** PHI when the health information can be linked to an individual.

Examples of PHI

- Names
- Social Security Numbers
- E-mail Addresses
- Date of Birth
- License Plate Number
- Geographic Subdivisions
(street address)
- Telephone Numbers
- Any unique characteristic or code which will link an individual to his or her health information



PHI Use versus Disclosure

- PHI is used when it is shared, examined, applied and analyzed
- PHI is disclosed when it is released, transferred, or accessed by anyone outside the NAF HBP and authorized employees

Treatment, Payment, and Health Care Operations (TPO)

Authorized Employees can use PHI for TPO Purposes:

- **“Treatment”** means the provision, coordination, or management of your health care by one or more health care providers, including consultation between providers and referrals from one provider to another.
- **“Payment”** is defined as activities undertaken by either-- the Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Plan; or health care provider or the Plan to obtain or provide reimbursement for the provision of health care.
- **“Health care operations”** means activities of the Plan, which are related to the function of the Plan. These activities include--quality assessment, improvement reviews; reviewing the competence or qualifications of health care providers; conducting or arranging for medical review, legal services, or auditing functions; business planning and development; and business management and general administrative activities, including customer service and resolution of internal grievances.

Specific Examples of Health Care Operations & Payment (Permitted PHI)

Health Care Operations

- Underwriting
- Premium rating
- Activities for obtaining, renewing or replacing a health insurance contract
- Auditing claims & deciding claims appeals
- Conducting quality assessment & case management

Payment Activities

- Determining eligibility or coverage
- Adjudicating a claim or appeal
- Determining medical necessity
- Utilization review
- Stop loss
- Coordinating benefits
- Subrogation

Examples of Using PHI for TPO purposes

- Enrolling employees into the NAF HBP or HMO
- Reviewing Explanation of Benefits forms to help an employee receive payment
- Examining data in a spreadsheet for overseeing the NAF HBP or HMO Plans
- Reviewing an Appeal
- Examining Provider Billing

Minimum Necessary Standard

- When at all possible, use/disclose PHI to the limited amount of health information or unique identifiers necessary in completing the job
- Example:
When an authorized employee is sharing a report for TPO purposes, remove all PHI not necessary in reviewing the report such as names, street addresses etc.

When to obtain an individual's authorization to use PHI

- Anytime PHI is used outside of TPO, authorized employees must obtain a signed Authorization Form from the individual
- Example:
A divorced individual requests a copy of their ex-spouse's PHI from their personnel file. Authorized employees can not provide that information without the ex-spouse's signed Authorization Form releasing that information

What is Included in the Authorization Form

Every authorized employee should have the Authorization Form in case a situation occurs when PHI needs to be released for reasons outside of TPO. One can not condition benefits on whether or not an individual signs an authorization form.

- The form describes the PHI to be used or disclosed
- Who will use or disclose PHI and for what purpose
- The individual's right to revoke the Authorization Form at any time
- An expiration date
- The signature of both the authorized employee and the individual to which the PHI pertains

When is an Authorization Form not required?

- Public health activities related to disease prevention
- To report victims of abuse, neglect or domestic violence
- For audits, legal investigations or law enforcement purposes
- To avert a serious threat to health and safety
- When the information has been de-identified and does not link or identify an individual to their health information

Revoking an Authorization Form

Employees have a right to revoke their authorization form at any time. Procedures for an individual who wants to revoke an Authorization Form:

1. Obtain a written signed letter from the individual requesting revocation
2. Attach revocation to original Authorization Form and keep in file
3. Cease using PHI for reasons other than TPO

Rights of Individuals under the Privacy Rule

Individuals have a right to:

- Receive a paper copy of the HIPAA Privacy Notice explaining their health plan's privacy policies and practices
- Access their own PHI
- Request amendments to their PHI in their personnel files etc.
- Request an accounting of their PHI disclosures (i.e., those outside the scope of TPO)
- File a complaint for PHI not being used in accordance with the Privacy Rule

HIPAA Privacy Notice

- The HIPAA Privacy notice was sent to all employees by April 14, 2003
- The HIPAA Notice informs employees that the NAF HBP is protecting health information
- The notice also describes the NAF HBP use of PHI and the employees rights under the Privacy Rule
- A paper copy of the notice must be given to employees upon request
- The notice is located at <http://crossroads/MRG/BenefitsDocs/DoD%20NAF%20Privacy%20Notice.pdf> for those that do not request a paper copy

Rights of Individuals to access/amend their own PHI

- The HIPAA Privacy rules allow individuals to inspect, amend, & copy PHI in their own personnel records.
- Requests to amend PHI must be in writing and state the reason for the amendment
 - Authorized employees act on the request no later than 60 days after receipt of such a request (if 60 days is not possible, only another 30 day extension is allowed)
 - Inform the individual that their amendment has occurred, or if the amendment is not feasible, contact the Privacy Official for guidance
 - Amendment will be included as an addition to, and not a replacement of, already-existing records

Individuals Right to Request an Accounting of PHI Uses/Disclosures

The HIPAA Privacy rules allow individuals to request an accounting of the uses/disclosures of PHI made by the Plan during the six years prior to a request, except for:

1. Treatment, payment and health care operations (TPO)
2. Disclosures to the individual to which the PHI applies
3. Disclosures pursuant to an individual's authorization
4. Disclosures to persons involved in care of individual
5. Disclosures for national security or intelligence purposes
6. Disclosures to correctional institutions or law enforcement
7. officials
8. Disclosures that occurred prior to 14 April 2003.

Disclosure of PHI to Family Members

- Authorized employees are generally not entitled to share PHI with an employee's family member(s)
- The exceptions to this rule are:
 - The family member or close personal friend is designated as the "Personal Representative" in a signed letter attached to an Authorization Form
 - The consent to disclosing PHI is due to an emergency

Disclosure of PHI to Bargaining Parties

- A bargaining party may request claims and financial information for review (negotiating plan design changes etc.) that has been de-identified
- Bargaining parties are not entitled to PHI without the individual's authorization form
 - De-identify any information released to bargaining parties



Role of the Privacy Officer

The privacy officer has ultimate responsibility for ensuring the NAF HBP is compliant with HIPAA Privacy Rules

Duties include:

1. Remain up-to-date on regulatory developments
2. Develop and implement covered entity's privacy policy, procedures, and notices
3. Oversee program compliance audits and monitoring
4. Designate contact person for receiving privacy complaints from individuals
5. Maintain records of policies and procedures
6. Develop and implement a HIPAA Privacy Rules training program for authorized employees

Role of the Privacy Official

- The Privacy Officer has designated contacts for the NAF HBP which are called Privacy Officials
- Questions and concerns outside the scope of this training may be discussed with your designated Privacy Official
- The HIPAA procedures guidelines is a good reference as well. Every effort has been made to make the guidelines complete, to include forms and instructions for day to day operations.

Individual's Right to a Complaint

If an individual believes their PHI has been used/disclosed in violation of the HIPAA Privacy Rules, they may file a complaint with the Office of Health and Human Services or the NAF HBP's Privacy Officer.

The final privacy rule is enforced by The Health & Human Services (HHS) Office of Civil Rights.

A complaint should be filed within 180 days of when the complainant knew or should have known that the act or omission occurred.

Complaints to the NAF HBP's Privacy Officer:

1. Inform the employee they there will be no retaliatory action against them for filing a complaint
2. Inform the employee that the complaint must be in writing
3. Send the complaint to:
Privacy Officer C/O DoD NAF Personnel Policy Office,
1400 Key Boulevard Suite B200, Arlington, VA 22209

Security of PHI

The proposed HIPAA Security Regulations require a covered entity to maintain reasonable and appropriate administrative, technical and physical safeguards to:

- Ensure integrity and confidentiality of information
- Protect against threats or hazards
- Safeguard against unauthorized uses or disclosures

Security of PHI

- Under the Privacy Rules, any use of PHI used electronically, paper based, faxed, orally, through voicemails or e-mail is protected.

Electronic Transactions include:

- Internet
- Private Networks
- Telephone Response Systems
- Fax machines
- E-mail
- Floppy Disks/ USB Drives/ CDs
- Copy machines

Ways to Secure PHI

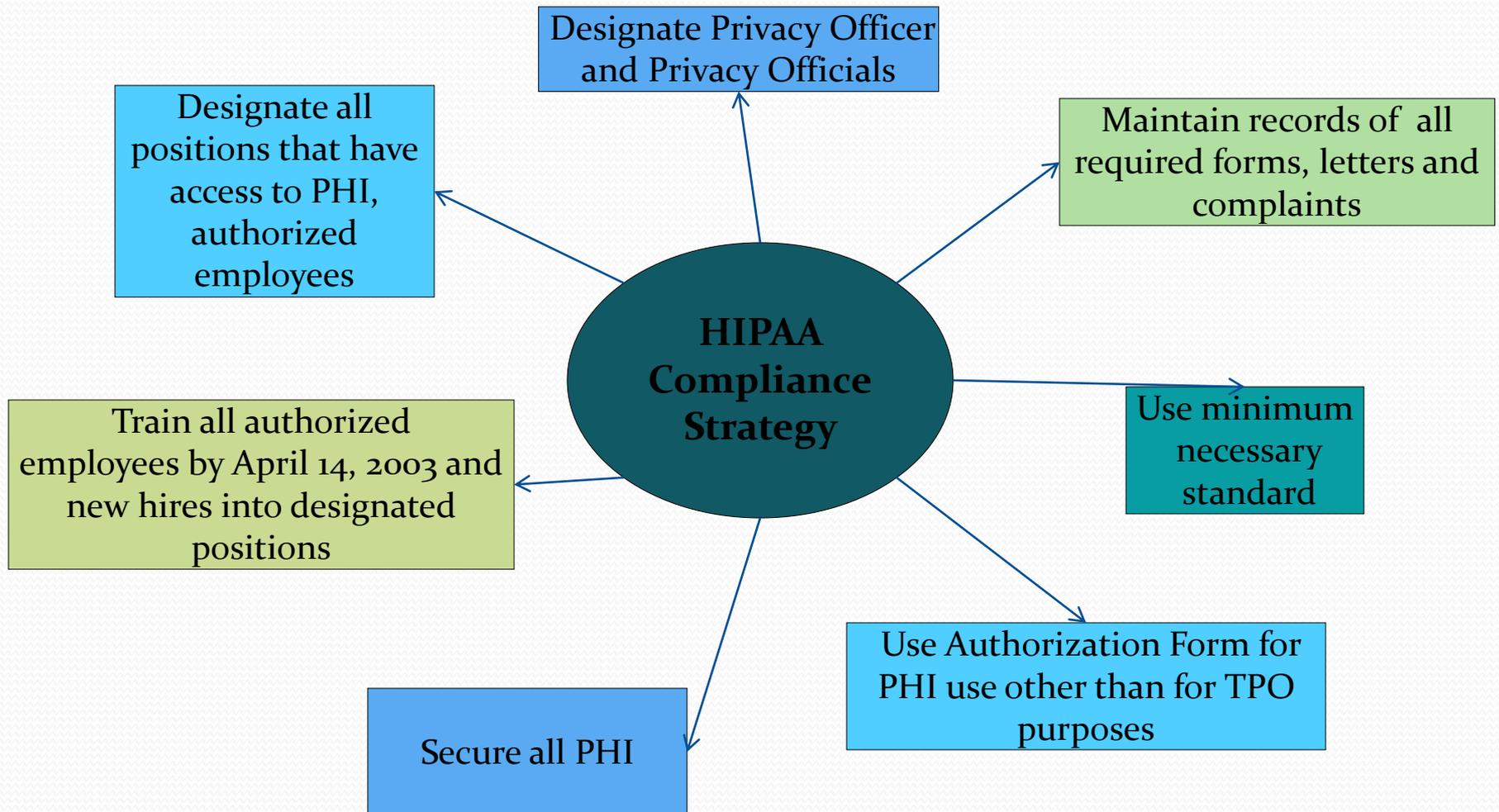
- Lock your computer station when you are not physically at your desk
- Do not leave voicemail messages with PHI
- Do not receive faxes containing PHI in public area without monitoring receipt of the fax
- Shred documents containing PHI before disposing of them
- Lock cabinets containing PHI
- Use the Minimal Necessary Standard when transmitting PHI through e-mail for TPO purposes
- Do not leave papers or floppy disks with PHI left unattended or unsecure on your workstation
- Destroy any documents containing PHI that are no longer needed
- Do not discuss PHI information over the phone if non-authorized employees are present (de-identify in these circumstances)



Documentation/Record keeping

- Documentation and records concerning HIPAA Privacy Rules will be kept for six years from its creation or April 14, 2003, whichever comes later
- Documents which must be kept in a secure location:
 1. Signed Authorization Forms
 2. Signed Revocation of Authorization Forms
 3. Complaints
 4. Letters requesting an amendment to individual's PHI
 5. Letters designating a Personal Representative

Compliance Strategy



Duty To Mitigate

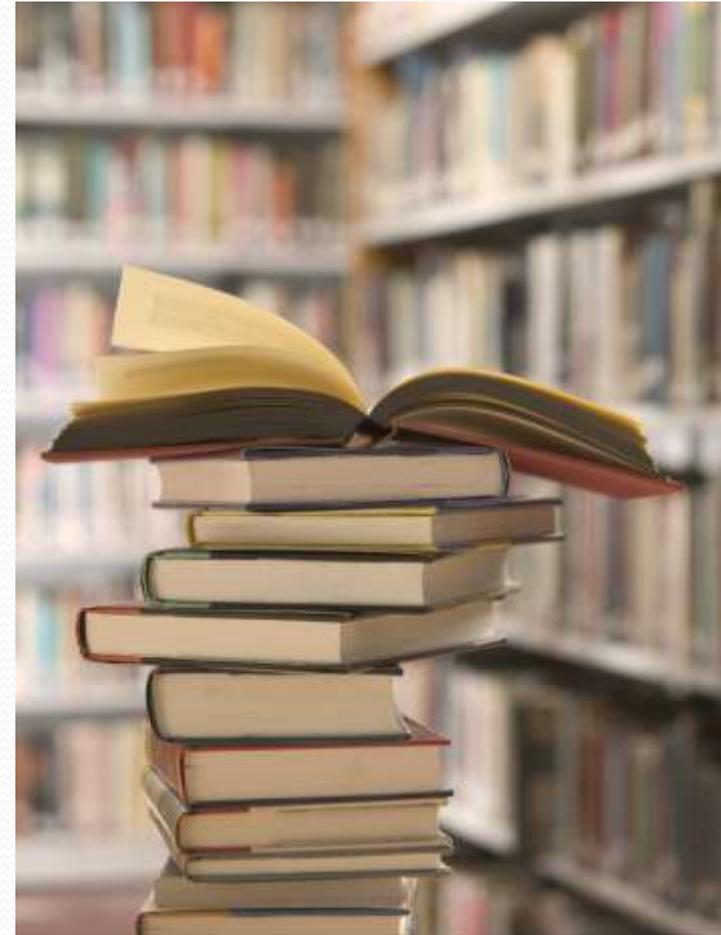
- If unauthorized disclosure occurs, then the NAF HBP must mitigate any harmful effects.
- Efforts include retrieving the information, putting procedures in place to prevent future occurrences, correcting system errors and additional training.

Other HIPAA Deadlines to Know

- HIPAA is requiring that Electronic Health Care Transactions use the same code set(s) and identifiers between entities
- Electronic Health Care Transactions
 - ASCA - Administrative Simplification Compliance Act governs covered entities such as health care clearing houses, insurance companies, hospitals etc
 - Deadline: October 16, 2003
- Electronic Health Care Transactions Standards cover:
 - Health claims, health care payments, COB, health claim status, enrollment or disenrollment, eligibility, premium payments, referrals, 1st report of injury, health claim attachments

Where to Get More Information

- Health and Human Services
<http://www.hhs.gov/ocr/privacy>
- Department of Labor
<http://dol.gov>
- HIPAA Procedures Guideline
- Privacy Official



Thank You for Taking HIPAA Privacy Rules Training

- Remember to take the HIPAA Training and turn into your local Privacy Official.
<http://crossroads/MRG/BenefitsDocs/HIPAAQuiz.doc>
- Keep the HIPAA Guidelines near your workstation for reference

Privacy is our Responsibility!

