Health Insurance Portability and Accountability Act (HIPAA) addresses the use and disclosure of individuals' health information (protected health information PHI). It became effective April 14, 2003/

Goal: Assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care to protect the public's health and well being.

Who is covered by the privacy rule?:

1. **Health Plans**
    a. Individual and group plans that provide or pay the cost of medical care
2. **Health care providers**
    a. Every health care provider, who electronically transmits health information in connection with certain transactions
        i. claims,
        ii. benefit eligibility inquiries,
        iii. referral authorization requests
3. **Health care clearinghouses**
    a. Entities that process nonstandard information they receive from another entity into standard format or data content
4. **Business associates**
    a. Person or organization that performs certain functions or activities on behalf of or to a covered entity that involve the use or disclosure of individually identifiable health information
        i. Janitorial services, attorneys, copying services
    b. At termination of contract, where feasible, all PHI must be returned to the entity

WHAT information is protected?

1. All individually identifiable health information held or transmitted by a covered entity or its business associate in any form or media, whether electronic, paper, or oral.
    a. The individual's past, present or future physical or mental health or condition
    b. The provision of health care to the individual, or
    c. The past, present, or future payment for the provision of health care to the individual
2. Information including
    a. Demographic data
    b. Name
    c. Birth date
    d. Social Security Number

WHEN can PHI be disclosed?

1. As the Privacy Rule permits or requires
    a. To individuals or their personal representative when authorized in writing
        i. Personal representative is to be treated the same as the individual and is a personal legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate
        ii. Parents are the personal representatives for their minor children
2. Health & Human Services when it is undertaking a compliance investigation
3. Entity is **permitted**, but **not** required, to use and disclose PHI without an individual's authorization in the following circumstances:
    a. To the individual who is the subject of the information
    b. For treatment, payment and health care operations
        i. Treatment: provision, coordination or management of health care and related services
        ii. Payment: activities to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits or obtain reimbursement
        iii. Health Care Operations
            1. case management
            2. competency assurance
            3. medical reviews, audits orlegal services
            4. specified insurance functions
            5. business planning, development, management
    c. Opportunity to agree or object
        i. Informal permission may be obtained by asking outright or by circumstances which give the opportunity to agree or object
    d. Incident to an otherwise permitted use and disclosure
        i. not every risk of an incidental use or disclosure of PHI be eliminated
            1. disclosure occurs as a result of an otherwise permitted use as long as reasonable safeguards are in place
    e. Public interest and benefit activities permitted not required)
        i. National priority purposes
            1. Required by law
            2. Public health activities (controlling disease, injury, abuse, neglect)
            3. Victims of abuse, neglect or domestic violence
            4. Health oversight activities (audits and investigations for oversight of system and benefit programs)
            5. Judicial and administrative proceedings (court order)

6. Law enforcement purposes
    a. Court orders, warrants, subpoenas
    b. Identify or locate a suspect, fugitive, material wines or missing person
    c. Request about victim of a crime
    d. Alert law enforcement of person's death is criminal activity suspected
    e. When PHI may be evidence of a crime on it's premises
    f. Medical emergency not occurring on its premises
7. Funeral directors as needed and to coroners or medical examiners to identify a deceased person
8. Organ and tissues donation
9. Research provided Internal Review Board approved
10. Serious treat to health or safety (imminent threat to person or public when made to someone who can prevent or lessen the threat)
11. Essential Government Functions
    a. Proper execution of military mission
12. Workers' Compensation

f. Limited data set for the purposes of research, public health or health care operations

4. Entity must obtain authorization to use and disclose PHI when information is not for treatment, payment or health care operations.
    a. Individual's written authorization must be obtained
    b. Authorization must be written in specific terms and in plain language.
        i. Information to be disclosed
        ii. The person disclosing
        iii. The person receiving the information
        iv. Date authorization is to expire
    c. Authorization can be revoked
        i. if action has not been taken
        ii. if authorization has expired
        iii. in writing
    d. Written authorization must be obtain to disclose psychotherapy notes
5. Limiting uses and disclosures
    a. Minimum necessary to accomplish intended purpose
        i. May not need entire medical record, just a portion
    b. Entity must restrict access based on specific roles of workforce
    c. Entity must establish policies and procedures for routine, recurring disclosures or request that limits the PHI to the minimum amount reasonably necessary
6. Notice and other Individual Rights

a. Entity must provide notice of its privacy practices.
    i. Describe ways entity may use and disclose PHI
    ii. State entity's duties to project privacy
    iii. Provide notice of privacy practices
    iv. Abide by the terms of the current notice
    v. Must describe individuals' rights including right to complain to HHS
    vi. Point of contact for further information and making complaints
    vii. May be changed if I have reserved this right in the notice
    viii. Distribution requirements
        1. Not later than first service encounter by
            a. Personal delivery
            b. Prompt mailing
            c. Web site, if have one
        2. Posting the notice in the office
        3. In emergency treatment situations, furnish as soon as practicable
        4. Must make good faith effort to obtain written acknowledgement of receipt of notice
b. Access to PHI
    i. Individuals have right to review and obtain a copy of their PHI in a designated record set
        1. Exceptions:
            a. Psychotherapy notes
            b. Information compiled for legal proceedings
            c. Laboratory results which CLIA prohibits access
            d. Information health by certain research labs
    ii. Entity may deny access under specific circumstances
        1. Believe access could cause harm to the individual or another
        2. In such situations individual must be given right to have denials reviewed by a licensed health care professional for a second opinion
    iii. Entity may impose reasonable, cost-based fees for the cost of copying and postage. Must notify of cost prior to release.
    iv. Individuals have the right to amend their PHI in a designated record set when that information is inaccurate or incomplete
        1. Request must be in writing
        2. Entity may accept or deny this request within 60 days
        3. Written denial must be provided
        4. Individual may submit a statement of disagreement for inclusion in the record
    v. Individuals have a right to an accounting of the disclosures of their protected PHI. Accounting must be retained for 6 years. Accounting NOT required

1. For treatment, payment, health operations
2. To the individual or their representative
3. For notification of or to persons involved in health care or payment
4. Pursuant to an authorization
5. Limited data set
6. National security
7. Correctional institutions or law enforcement regarding inmates or those in lawful custody
8. incident to otherwise permitted or required uses

vi. Individuals have the right to request entity restrict use or disclosure of PHI
    1. for treatment, payment or health care operations
    2. disclosure to persons involved in the individuals' health care or payment of health care
    3. disclosure to notify family memers or others about the individual's general condition, location or death
    4. Entity is under no obligation to agree to the requests for restrictions
    5. If entity does agree, must comply with the restrictions

vii. Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information

7. Administrative Requirements
    a. Entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule
    b. Identify the internal and external risks of disclosure of PHI
    c. Create and implement a plan to reduce the risk of releasing PHI
    d. Entity must monitor the implementation and enforce any breaches of policy.
    e. Entity must designate a privacy official responsible for developing and implementing privacy policies and procedures and a contact person or contact office responsible for receiving complains and providing individuals with information on entity's privacy practices
    f. Workforce members including employees, volunteers, trainees must be trained on privacy policies and procedures prior to April 14, 2003
    g. Entity must mitigate to the extent practicable any harmful effect is learns was caused by use or disclosure of PHI by its workforce or its business associates in violation of the privacy policies and procedures
    h. Entity must maintain reasonable and appropriate administrative, technical and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule
        i. Shredding documents containing PHI before discarding them

        ii. Securing medical records with lock and key
        iii. Limiting access to keys and pass code
    i. Entity must have procedures for individuals to complain about its compliance. Complaints need not be made directly to the entity.
        i. Complaints validated by the HHS may results inn a compliance review.
    j. Entity may not retaliate against a person for exercising rights provided in the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority
    k. Entity must maintain for six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints and other action, activities and designations.
8. State Law – when state laws are contrary to the Privacy Rule, federal requirements will apply
9. Enforcement and Penalties for noncompliance
    a. HHS will seek the cooperation of covered entities and may provide technical assistance to help in compliance
    b. HHS may impose civil money penalties of
        i. $100 per failure to comply with the Privacy Rule
        ii. Penalty may not exceed $25,000 per year for multiple violations in a calendar year
        iii. HHS may not impose civil money penalty when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation
    c. Criminal penalties imposed when a person knowingly obtains or disclosed individually identifiable health information in violation of HIPAA faces:
    d. $50,000 and up to one year imprisonment
    e. Penalties increase to $100,000 and up to 5 years imprisonment if the wrongful conduct involves false pretenses
    f. Up to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain, or malicious harm