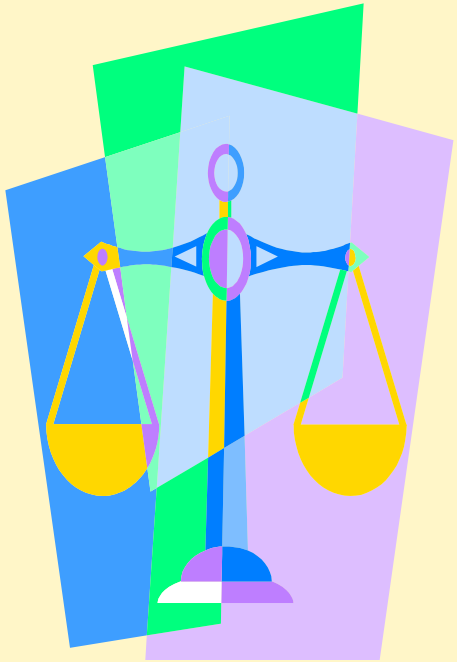
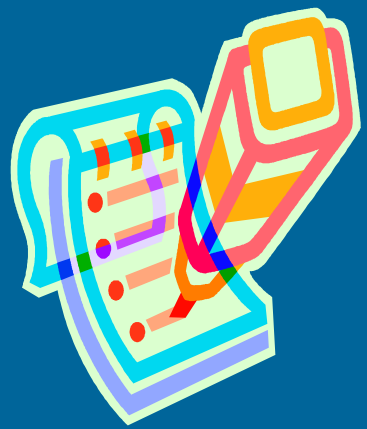


Administrative Requirements



United States Department of Health & Human Services

Policies and Procedures

- Implement policies and procedures regarding PHI that are designed to comply with the Privacy Rule
  - Change policies and procedures as necessary to comply with applicable laws
  - Ensure that material changes to privacy practices are stated in the notice

Safeguards and Mitigation

- Implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI
- Mitigate any harmful effect of an use or disclosure of PHI in violation of its policies and procedures or the Privacy Rule that is known to the Covered Entity, to the extent practicable

Workforce Training and Employee Sanctions

- Provide privacy training to all of its workforce, as necessary and appropriate to their functions
- Develop and apply a system of sanctions for employees who violate the entity's policies or the requirements of the Privacy Rule

45 CFR §164.530(b), (e)

Personnel Designations

- Designate a privacy official
  - Responsible for privacy policies and procedures
- Designate a contact person or office responsible for receiving complaints

Complaint Process and No Waiver or Retaliatory Acts

- Provide a process for individuals to make complaints to Covered Entity
- Do not require individuals to waive their rights to file a complaint with the Secretary or their other rights under Privacy Rule
- Refrain from intimidating or retaliatory acts

45 CFR §164.530(d), (g)

Documentation Requirement

- Documentation requirements – written or electronic for 6 years. Examples include:
  - Policies and Procedures
  - Training provided, Privacy Official, Contact Person
  - Complaints to Covered Entity and their disposition, if any
  - Notice of Privacy Practices, Acknowledgement, and Good Faith efforts to obtain Acknowledgments
  - Authorizations
  - Business Associate Contracts
  - IRB/Privacy Board Waivers
  - Designated record sets that are subject to access by the individual, access contact persons, requests, and responses

Documentation Requirement

- Amendment contact persons, requests, denials, disagreements and rebuttals
- Information required to be in accounting, accounting contact person, requests, and accountings provided to individual
- Restriction Request Agreements
- HCC Designations
- Affiliated Covered Entity Designations
- Certification of Group Health Plan document amendment
- Verification documents of public officials, personal representatives, etc.
- Any other communication required by Rule to be in writing

Applicability to Group Health Plans

- A Group Health Plan that
  - provides all health benefits through issuer or HMO and
  - does not create or receive PHI other than summary health information or enrollment/disenrollment information is
- Not subject to the requirements of this section except:
  - prohibiting waiver of rights,
  - prohibiting retaliation and intimidation and
  - documenting plan amendments

Common Compliance Issues to Consider

- Determine if you are a Covered Entity
- Decide on organizational structure
- Identify Business Associate relationships and enter Business Associate Agreements
- Compare current PHI use and disclosure practices with Privacy Rule requirements, and identify where practices need to change. Identify "TPO" uses and disclosures of PHI, all other uses and disclosures (e.g., public policy), and develop Minimum Necessary policies and protocols
- Develop a valid authorization form for future use

Common Compliance Issues to Consider

- Develop and provide a Notice and, if necessary, an Acknowledgment form
- Develop a system to track and account for disclosures
- Designate a Privacy Official and contact person or office
- Design and Implement Policies and Procedures
- Develop and implement systems to safeguard PHI
- Train workforce
- Check the Rule for particular requirements