Working with the HIPAA Privacy Manual and Forms

HIPAA Summit West II

Clark Stanton & Tom Jeffry
Davis Wright Tremaine LLP

Table of Contents

- Introduction
- HIPAA Basics
- Preemption and Interaction with State Law
- Interface with HIPAA Security Requirements
- Special Topics: Health Research
- Release of Information
- Business Associates
- Patient Rights
- Notice of Privacy Practices
- Administrative Requirements
- Privacy Officer
- Personnel
- Enforcement of HIPAA

HIPAA Basics

Administrative Simplification Provisions of HIPAA

- Transactions
  - Final standards effective October 2003
- Privacy
  - Final standards effective April 2003
- Security
  - Proposed standards published August 1998
  - Final standards expected this year

Covered Entities

- Health Plans
  - Plans that provide or pay for medical care
- Health Care Clearinghouses
  - Entities that process or facilitate processing non-standard data elements into standard data elements, or vice versa
- Providers who transmit data electronically
  - Furnishes, bills or is paid for health care in the normal course of business

Privacy — General Rule

- A covered entity may not use or disclose Protected Health Information except:
  - For treatment, payment or health care care operations
    - Providers usually require a general written "consent"
  - Without consent or authorization, for governmental and other specified public interest purposes
  - Pursuant to individual "authorization"

Protected Health Information

- "Protected health information" —
  - Individually identifiable health information
  - In whatever form it exists
    - Electronic, written, oral
  - But not "de-identified" information

Protected Health Information

- Individually identifiable health information —
  - Information relating to —
    - An individual's health or condition
    - Provision of health care to an individual
    - Payment for health care to an individual
  - Identifies an individual, or there is a reasonable basis to believe it can be used to identify an individual

De-Identification

- Confidentiality requirements do not apply to health information that has been “de-identified”
- Qualified person must determine that risk of re-identification is “very small”
- Removal of specified identifiers creates presumption of de-identification

De-Identification

- Information is presumed de-identified if —
  - The following identifiers are removed or concealed:

Name	Address	Relatives	Employer
Dates	Telephone	Fax	e-mail
SSN	MR #	Plan ID	Account #
License #	Vehicle ID	URL	IP address
Fingerprints	Photographs	Other unique identifiers	

  - And the CE does not have actual knowledge that the recipient could use it to identify the individual

Required Disclosures

- To the individual, pursuant to request
- To the Secretary of DHHS, to determine compliance

Permitted Disclosures

- A covered entity may not use or disclose Protected Health Information except:
  - For treatment, payment or health care care operations
    - Providers usually require a general written "consent"
  - Without consent or authorization, for governmental and other specified purposes
  - Pursuant to individual "authorization" for other purposes

Disclosures Requiring Consent Treatment

- Treatment includes —
  - Provision of health care
  - Coordination of health care
  - Referral for health care

Disclosures Requiring Consent Payment

- Payment includes —
  - Health plan activities to determine payment responsibilities and make payment
  - Provider activities to obtain reimbursement
  - Such as —
    - Coverage determinations
    - Billing and claims management
    - Medical review, medical data processing
    - Review of services for medical necessity, coverage, appropriateness; utilization review

Disclosures Requiring Consent Health Care Operations

- Health care operations include —
  - Quality assessment and improvement
  - Peer review, education, accreditation, certification, licensing and credentialing
  - Insurance-related activities
  - Auditing and compliance programs
  - Business planning and development
  - Business management and general administration

Notice of Privacy Practices

- Provider's routine uses/disclosures of PHI
- Description of patient rights (next slide)
- Provider duties (e.g., abide by terms of notice)
- How to file a complaint w/ provider/DHHS
- Contact information

Patient Rights

- Right to inspect and copy PHI
- Right to amend (if info is incorrect or incomplete)
- Right to accounting of non-routine disclosures of PHI
- Right to request additional restrictions on use/disclosure
- Right to request confidential communications of PHI
- Right to written notice of how provider will use/disclose PHI (copy of NPP)
- Right to authorize release for non-routine use/disclosure; consent to routine use/disclosure (~health plans)

Consent Requirements

- Required at outset of care or enrollment
- Covers treatment, payment and health care operations
- Inform patient of:
  - CE's privacy practices
  - Right to request additional restrictions
  - Right to revoke consent for future actions
- Signed and dated

Consent Requirements

- May not be combined with notice of privacy practices
- May be combined with informed consent if
  - Visually separate
  - Separately signed
- Joint consents prohibited except for organized health care arrangements that share a privacy notice

Consent Requirements

- Exceptions —
  - Indirect treatment relationship
    - Delivers care on orders of another provider
    - Reports to the other provider
  - Provider unable to obtain consent:
    - Emergencies
    - Communication barriers, but consent can be inferred
    - Legal obligation to treat
    - Provider must document attempt to obtain consent

Disclosures Requiring Oral Agreement

- Individuals must have opportunity to agree or object to certain uses or disclosures of PHI:
  - Directory (name, location, general condition & religious affiliation)
  - Disclosure to family/friends involved in patient's treatment of PHI directly related to their involvement
  - Notification to responsible person about location, general condition or death
- If the individual objects, CE may not disclose

Permitted Disclosures Government and Other Purposes

- As required by other laws
- Public health activities
- Victims of abuse, etc.
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement purposes
- Decedents — coroners and medical examiners
- Organ procurement
- Research purposes, under limited circumstances
- Imminent threat to health or safety (to the individual or the public)
- Specialized government function
- Workers' compensation

Authorization

- CEs must obtain express authorization for disclosure of PHI not covered by "consent" or otherwise authorized by HIPAA
- Authorization must be in writing using forms meeting specific requirements
  - Model forms in the proposed rule were withdrawn
- CE may *not* condition treatment on "authorization" — except for clinical trials
- Authorization is revocable at will

Permitted Disclosures Individual Authorization

- Required elements--
  - Meaningful and specific description of information
  - Identity of persons authorized to make disclosure (may be by class)
  - Specific identity of persons to whom disclosure may be made
  - Date and signature
  - Expiration date
  - Where authorization requested by CE —
    - Description of purpose of request
    - Statement of financial gain

Permitted Disclosures Individual Authorization

- Other rules--
  - CE may condition treatment or enrollment on "consent"
  - CE may not condition treatment on "authorization" for other purposes, except for clinical trials
  - Authorization and consent are revocable at will, except to the extent the entity has relied on them

Authorization

Psychotherapy Notes

- A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:
  - (i) To carry out the following treatment, payment, or health care operations, consistent with the requirements for consent:
    - Use by originator of the psychotherapy notes for treatment;
    - Use or disclosure by the CE in training programs, or
    - Use or disclosure by the CE to defend a legal action or other proceeding brought by the individual; and

Authorization

Psychotherapy Notes

- A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except: (cont'd)
  - (ii) A use or disclosure under the following circumstances:
    - to the individual
    - required by law (e.g., abuse reporting, judicial proceedings, law enforcement purposes)
    - for oversight of the originator of the psychotherapy notes
    - to a coroner or medical examiner, or
    - is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public

Minimum Necessary Information

- CE must make reasonable efforts to limit uses, disclosures and requests for PHI to the minimum necessary
- Exceptions:
  - Disclosure to a provider for treatment
  - Disclosure to individual
  - Disclosure to DHHS for HIPAA compliance
  - Disclosure required by law

Minimum Necessary Information

- Uses of PHI. CE must:
  - Identify persons or classes of persons who need access to PHI
  - Identify their need for health information and the conditions to access
  - Limit access accordingly
- Disclosures of and requests for PHI. CE must:
  - Implement policies to limit routine disclosures and requests
  - Review non-routine disclosures and requests individually

Minimum Necessary Information

- CE may rely on scope of information requested by —
  - A public official
  - Another covered entity
  - A “professional” providing services to the CE
  - Researchers (as long as the research requirements are satisfied)
- A CE may not disclose the entire record, unless it is specifically justified
  - But this does not apply to disclosure to providers for treatment

Marketing

- No authorization required for —
  - Face-to-face encounter
  - Marketing concerning products or services of nominal value
  - Marketing concerning health-related services

Marketing

- Communications for health-related services must —
  - Identify covered entity
  - Disclose remuneration
  - Contain opt-out (except for general newsletters)
  - If targeted based on health condition —
    - Be based on determination of benefit to patient
    - Explain why the individual has been targeted

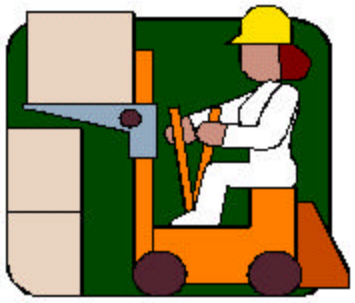
ACME Hospital

Dear Mrs. Jones:

Would you like to by a Forklift?

Your special price is only

$399.95.



You have been selected for this special offer because: your hernia makes it unsafe for you to lift heavy objects.

P.S. If you do not want to get advertisements from us, call 1-800-GET LOST.

P.P.S. We are getting money for sending this to you.

Fundraising

- CE may use or disclose to BA or related foundation for purposes of raising funds for CE's benefit —
  - Demographic information
  - Dates of health care provided
- CE must include opt-out information in fund-raising materials

ACME Hospital

Dear Mrs. Jones:

We hope you enjoyed your hernia operation.

Please consider making a donation.

P.S. If you do not want to get advertisements from us, call 1-800-GET LOST.

ACME Hospital

Dear Mrs. Jones:

Happy 90th birthday!

Have you remembered us in your will?

P.S. If you do not want to get advertisements from us, call 1-800-GET LOST.

Special Rules: Organizational Requirements

- Hybrid entities
- CEs with multiple covered functions
- Affiliated covered entities
- Organized health care arrangements
- Group health plans

Special Rules: Organizational Requirements

- **Hybrid entity**
  - Covered entity whose covered functions are not its primary functions
  - Covered with respect to its health care component
  - May not disclose PHI to other components, except as permitted to third parties (but it doesn't need BA agreements among its components)
  - Must designate health care components

Special Rules: Organizational Requirements

- Covered entities with multiple covered functions
  - Must comply with the requirements for each function
  - May disclose PHI only as necessary for the function for which the disclosure is made

Special Rules: Organizational Requirements

- **Affiliated Covered Entities**
  - Separate covered entities under common ownership or control may designate themselves a single covered entity
    - Ownership means an interest of 5% or more
    - Control means significant influence

Affiliated Entities

- Covered entities joined through common ownership or control
- Affiliated covered entities may:
  - Act as a single covered entity with a single compliance program
  - Appoint a single privacy officer
  - Utilize centralized reporting mechanisms
  - Adopt a single Notice of Privacy Practices
  - Adopt single consent and authorization forms
- Do not assume that affiliated covered entity status will always be desirable, even if it is available.

Affiliated Entities

- To qualify as affiliated entities:
  - Must meet the definition of a “covered entity”
  - Must be a distinct legal entity
  - Must share common ownership or control
- Common ownership means an ownership or equity interest of 5% or more
- “Common control” not so clearly defined:
  - “the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.”
- Hospital chain example.

Special Rules: Organizational Requirements

- **Organized Health Care Arrangements**
  - Clinically integrated care setting in which individuals typically receive health care from more than one provider.
  - Certain relationships between a group health plan and HMOs, health insurers and/or other group health plans.
  - An organized system of health care in which the covered entities:
    - Hold themselves out to the public as participating in a joint arrangement; and
    - Participate in joint UR, QA or payment activities.

Organized Health Care Arrangements

- Examples:
  - Hospital and its medical staff
  - Staff-model HMOs
  - Independent practice association
  - Medical group

Organized Health Care Arrangements

- Unlike affiliated covered entities, not treated as a single covered entity.
- Entities may share PHI for treatment, payment and operations without business associate agreements.
- May use a single Notice of Privacy Practices and joint consent form.

Special Rules: Organizational Requirements

- **Group health plans**
  - Plan documents must restrict disclosure of PHI to sponsor by plan and insurer/HMO
  - Plan may disclose summary health information for —
    - Obtaining premium bids
    - Modifying or terminating the group health plan

Special Rules: Organizational Requirements

- **Group Health Plans** (cont'd)
  - Other disclosures to plan sponsor
    - Limited to plan administration functions
    - Must be pursuant to assurances relating to use and disclosure (like BA agreement)
    - No use for employment-related actions
    - "Adequate separation" between plan and sponsor

Special Rules: Administrative Procedures

- CEs must have policies, procedures, and systems to protect health information and individual rights.
  - Designation of a privacy officer and contact person
  - Privacy training for workforce
  - Administrative and technical safeguards to prevent intentional or accidental misuse of PHI
  - Means for individuals to lodge complaints
  - Sanctions for employee violations
  - Mitigation procedures

How to Get Started

The 5 Stages of HIPAA

- Denial
- Anger
- Bargaining
- Depression
- Acceptance

Strategic Planning

- Board of Directors and senior management should be involved in high-level decisions, such as:
  - Organizational structure (if applicable)
  - Designation of privacy and security officers and related committees
  - Role of legal counsel
  - Funding

Getting Started

- Designate a privacy official
  - Identify job responsibilities and reporting relationships
  - See AHIMA sample job description in Manual
- Designate a security official
  - May, but need not be, the privacy officer

Privacy Officer

- In larger organizations, Privacy Officer and Security Officer should probably be two different people
- Privacy Officer responsible for access to, and uses and disclosures of, PHI
- Interaction with department, committee and clinical personnel

Security Officer

- Responsible for knowledge of network and enterprise-wide information systems and architecture, including:
  - Security threats and mechanisms
  - Intrusion management
  - Firewall administration
  - Incident response
  - Activity monitoring and auditing

Organize a Privacy Committee

- HIPAA compliance is an organization-wide effort

- Possible members of a privacy committee:
  - Privacy officer
  - Compliance officer
  - Internal auditor
  - Medical staff coordinator

Organize a Privacy Committee

- Risk manager
- Director of contracting
- Director of financial services
- Director of health information
- Director of human resources
- Director of information technology
- Director of nursing
- Director of public affairs

Organize a Privacy Committee

- Privacy Committee has a big job:
  - Review and assess current privacy practices
  - Determine what new policies and procedures are needed
  - Write new policies and procedures
- Privacy Officer cannot be the only person who understands HIPAA

Inventory of Information Practices

- Committee should begin by inventorying the ways that your organization uses and discloses PHI.
- Each use and disclosure must be evaluated to determine if it:
  - Is permissible without further consent or authorization
  - Complies with “minimum necessary” standard

Policies and Procedures

- New policies and procedures will need to be developed for:
  - Creating, distributing, retaining, storing, retrieving and destroying records that contain PHI
  - Notifying patients of privacy practices
  - Monitoring HIPAA compliance
  - Processing complaints about privacy violations
  - Entering into contracts with business associates
  - Sanctioning HIPAA violators
  - Protecting HIPAA complainants against retaliation.

Policies and Procedures

- Policies and procedures must be maintained in written or electronic form (can't just "do the right thing").

- Must retain policies and procedures for six years from date of creation of last effective date, whichever is later.

Workforce Training

- Privacy and security awareness training for:
  - Entire workforce by compliance date
  - New employees following hire
  - Affected employees after material changes in policies
- Document Training

Workforce Training

- "Workforce" includes employees, volunteers, trainees and others whose work is under the provider's control.
- Hospital medical staff are not workforce, but privacy training for physicians is advisable.
- Method of training is not specified (videos, handouts, tapes, etc.)

Workforce Sanctions

- Providers must develop sanctions for employees and other workforce members who violate policies and procedures.
- Sanctions should:
  - Be consistent with existing disciplinary requirements.
  - Be consistently enforced
  - Distinguish between major and minor infractions.

Workforce Sanctions

- Sanctions do not apply to whistleblowers.
- Breaches by business associates should be addressed in business associate agreement.

Security Standards

- Applies to health information whether or not identifiable:
  - Administrative procedures
  - Physical safeguards
  - Technical security services
  - Technical security for network communications

HIPAA Security

- The HIPAA statute requires covered entities to :
  - "maintain *reasonable* and appropriate administrative, technical and physical safeguards ... To *ensure* the integrity and confidentiality of [PHI] ..."
- Do you put the emphasis on "reasonable" or "ensure"?
  - In terms of dollars spent on IT upgrades, the difference can be huge.

HIPAA Security

- Did HHS intend to apply Pentagon-level security to a two-physician medical office?
- HHS has emphasized “reasonableness” in public statements.
- The proposed Security Rule offers a useful example involving a “small or rural provider” — a physician office with 1-4 physicians, 2-5 employees.

HIPAA Security Physician Office

- PC-based practice management system.
- Does not employ a systems administrator (too small).
- Self-certify that appropriate security is in place using a knowledgeable staff person or consultant.
- Assess risks and develop policies and procedures to address them.

HIPAA Security Physician Office

- Security configuration management
  - Can rely on features of purchased hardware and software, like virus protection software
- Activate internal auditing capabilities of software to track access to data
- Use locked rooms or closets to secure equipment and disks

HIPAA Security Physician Office

- Locate terminals in areas where public may not access
- User-based data access (user name, password approach)
- Use encryption for Internet transmission of PHI
- Chain of trust agreement with third party handling claims processing

Preemption:

How It Works
and
The Fun We'll Have

Preemption under HIPAA

- HIPAA:
  - Public Law 104-191; Section 1178:

    HIPAA (any provision, requirement, standard or implementation specification of HIPAA) shall supersede any contrary provision of State law.

- Preemption applies to all of HIPAA, not just the privacy portion

Exceptions to Preemption

- State laws addressing controlled substances
- Where **DHHS** determines a State law is **necessary** —
  - To prevent fraud and abuse
  - To ensure appropriate regulation of health plans
  - For reporting on healthcare delivery or costs
  - To serve a ***compelling need*** related to public health, safety or welfare
    - DHHS must determine invasion of privacy is warranted when balanced against the need.

Exceptions to Preemption

- **Public health laws** for reporting disease, injury, child abuse, birth or death, or public health surveillance, investigation or intervention

- Laws requiring **health plans** to report or provide access to information for audits, program monitoring, or facility or individual licensure or certification.

- Laws relating to the privacy of health information that are ***contrary to*** and ***more stringent than*** the HIPAA requirements

Preemption: Contrary

- **Contrary** means —
  - Covered entity could not comply with both State law and the HIPAA requirement

or

  - State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of HIPAA

Preemption: More Stringent

- **More stringent** means that State law —
  - Has stricter limits on use or disclosure of health information
    - Except for disclosures to DHHS or patient
  - Gives greater rights of access to or correction of health information by the patient
    - Does not affect State laws authorizing or prohibiting disclosure of information about a minor to parent or guardian
  - Has harsher penalties for unauthorized use or disclosure

Preemption: More Stringent

- Provides greater information to individuals regarding use, disclosure, rights or remedies
- Has stricter requirements for authorizing or consenting to the disclosure of information
- Has stricter standards for record-keeping or accounting for disclosures of information
- With respect to any other matter provides greater privacy protection to the patient

Requesting Exceptions

- Process for requesting exceptions from DHHS
  - Anyone may request an exception
    - Request by a state must be submitted through its chief elected official or designee
- Some preemption issues will ultimately be determined through dialogue between state government and DHHS

How Preemption Will Work

- Preemption will focus on specific elements and aspects of State laws
  - HIPAA will be the baseline
  - State law will be given effect only to the extent that (a) there is no HIPAA law on the issue; (b) State law is more stringent; or (c) there is an exception
  - Exemptions will apply to specific State laws, not entire State schemes

How Preemption Will Work

California Example:

- No California equivalents for —
  - Business associates
    - CEs must contract with entities that receive PHI in order to perform service for/on behalf of CE
  - Minimum necessary
    - CEs should not ask for or release more than the minimum necessary PHI required for the purposes for which release is sought

How Preemption Will Work

California Example:

- No California equivalents (cont'd) —
  - Notice to patient of CE practices with respect to its handling of PHI
    - No notice requirement in CA law
  - Requirement of patient consent for use of PHI for treatment, payment and operations
    - California permits disclosure for such purposes without patient authorization or notice

How Preemption Will Work

California Example:

- Key California provision for preemption analysis purposes
  - Civil Code section 56.10(c)(14):
    - Information may be disclosed when the disclosure is otherwise specifically authorized by law

- This provision will permit the disclosure of health information that is permitted by HIPAA when there is question whether it is allowed under CA law

Business Associates

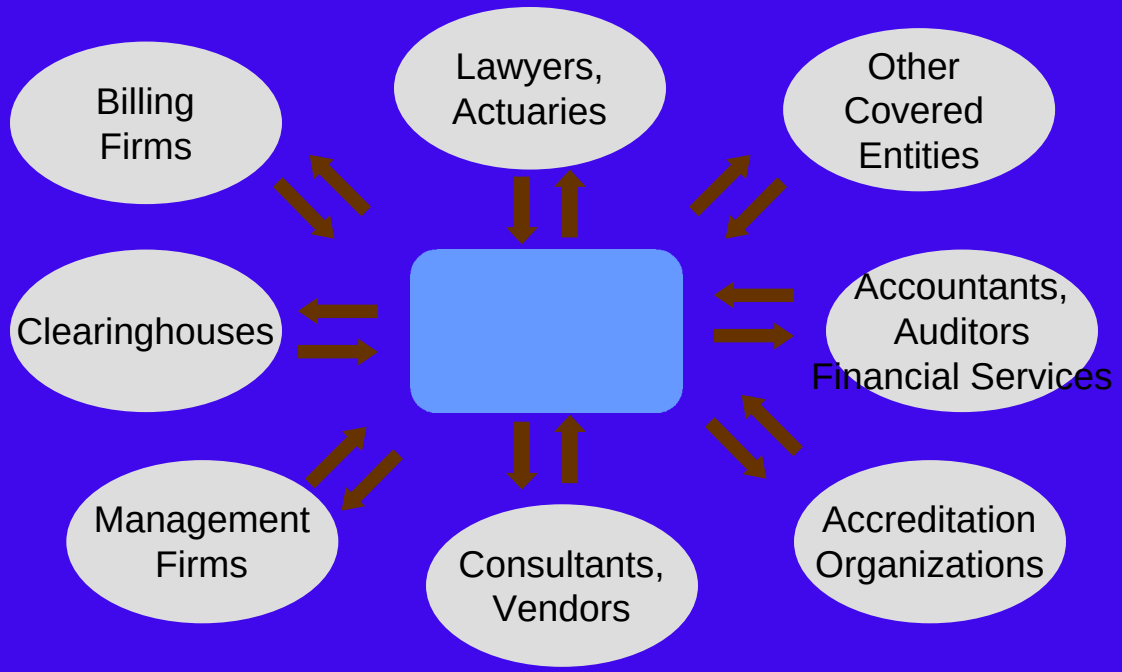
Business Associates
Satisfactory Assurances

- A covered entity may disclose protected health information to business associates if it obtains "satisfactory assurances" that business associates will appropriately safeguard the information

- Business associate contract required

Use and Disclosure — Who Is a Business Associate?

- A person who receives individually identifiable health information and —
  - On behalf of a covered entity performs or assists with a function or activity involving use or disclosure of information or otherwise covered by HIPAA
  - Provides certain identified services to a covered entity
- May be a covered entity

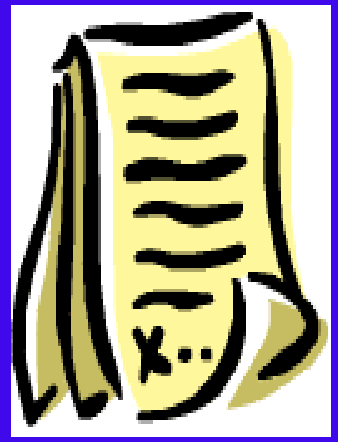


No Business Associate Relationship

- Health plan provides member info to pharmaceutical company to market drug
- Hospital contracts with bank to process credit card payments
- Medical group uses courier services to deliver medical records to laboratory

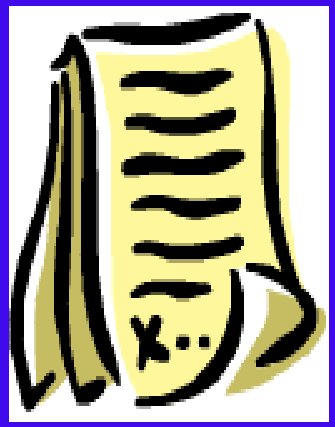
Use and Disclosure — Business Associate Contracts

- A covered entity may disclose protected health information to business associates if it:
  - Obtains "satisfactory assurances" that business associates will appropriately safeguard the information
- Business associate contract required
- Form agreement included in manual
  - Informational purposes/not legal advice
  - Any form must be adapted and individualized



Business Associate Contracts — Required Terms

- Use and disclose information only as authorized in the contract (Sections 2(a), 2(b))
  - No further uses and disclosures
  - Such uses and disclosures may not exceed what the covered entity may do under HIPAA
  - Data aggregation services exception
- Implement appropriate privacy and security safeguards (2(c))
- Report unauthorized disclosures to covered entity (2(d))
- Make available protected health information under access, amendment and accounting of disclosures rights (2(f), 2(g), 2(h))
- Incorporate any amendments to PHI

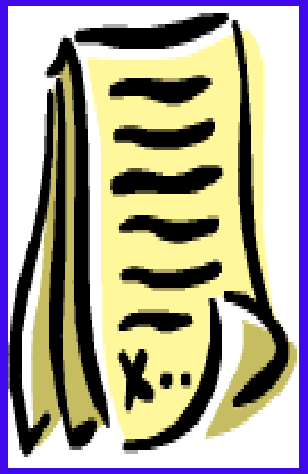


Business Associate Contracts — Required Terms

- Make available its records to HHS for determination of covered entity's compliance (2(i))
- Return/destroy protected health information upon termination of arrangement, if feasible (4(d))
- Ensure agents and subcontractors comply (2(e))
- Authorize termination by covered entities (4(a))

Business Associate Contracts — Provisions to be Considered

- Right to review contracts between business associates and their subcontractors/agents
- Business associate's insurance (2(m))
- Indemnification (5)
- Use for management and administration (2(a), 2(b))
- Effective date and "placeholder" provisions

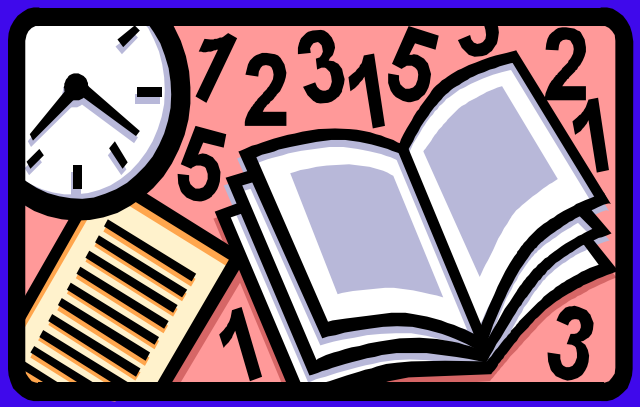


Liability for Business Associates

- If covered entity knows of a pattern of activity constituting a breach by the business associate, then
  - Must take reasonable steps to
    - Cure the breach or
    - End the violation
  - If unsuccessful,
    - Must terminate if feasible or
    - Report to DHHS
- Reprieve from proposed regulations
- Substantial and credible evidence standard

Business Associate Considerations

- Identify likely business associates
  - Start by listing everyone who receives individually identifiable health information
  - Determine who is/likely to be a business associate
- Allow for educational lead time



Enforcement

Enforcement - Penalties

- CMPs against persons who fail to comply
  - $100 per violation, not to exceed $25,000/year
- Criminal penalties for knowingly disclosing or obtaining PHI or using a unique health ID
  - Knowing only: $50,000, 1 yr, or both
  - False pretenses: $100,000, 5 yrs or both
  - Use for ***commercial or personal gain*** or malicious harm: $250,000, 10 yrs or both

Enforcement - Process

- Authority to impose civil money penalties has been delegated to the DHHS Office for Civil Rights
- Individuals may file complaints with DHHS/OCR, which will investigate
- DHHS/OCR may also conduct periodic HIPAA compliance reviews
- HIPAA provides no private right of action
  - But state law may authorize private actions

Working with the HIPAA Privacy Manual and Forms