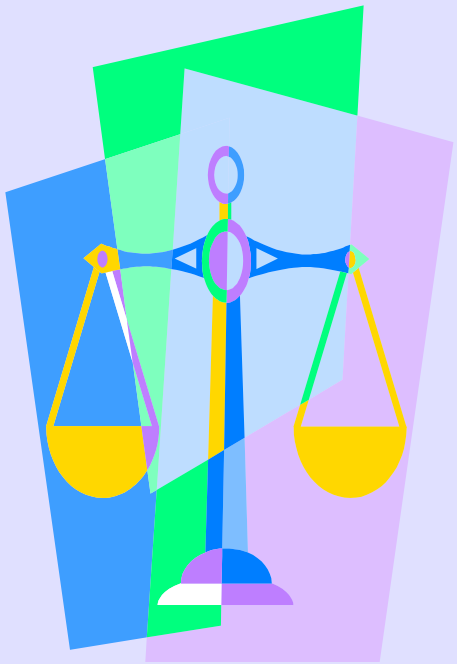
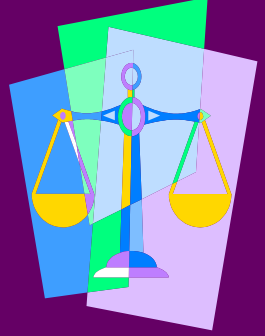


HIPAA Privacy Rule

National Conferences 2003

United States Department of Health & Human Services



"HIPAA"

The Health Insurance Portability and Accountability Act of 1996

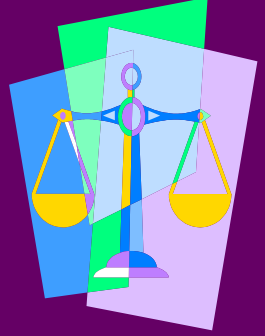
(Public Law 104-191)

Signed August 21, 1996

Title II

Subtitle F - Administrative Simplification

42 USC 1320d



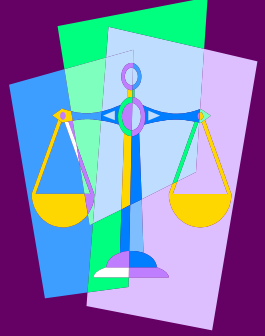
Purpose of HIPAA Provisions

Improve efficiency and effectiveness of health care system

by standardizing

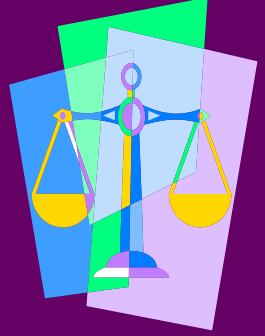
the electronic exchange of administrative and financial data

42 USC 1320d



Mandated Standards

- HHS was mandated to adopt of develop:
  - Specific transaction standards (claims, enrollment, etc.) including code sets
  - Security and electronic signatures
  - **Privacy**
  - Unique identifiers (including allowed uses) for employers, health plans, and health care providers

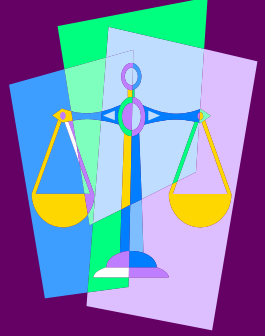


Privacy Rule

"Federal Floor" of Privacy Protections

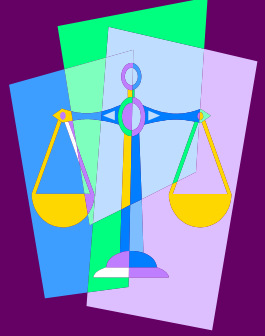
- First comprehensive federal health privacy protections
- "More stringent" state privacy protections remain in force

45 CFR § 160.202, § 160.203



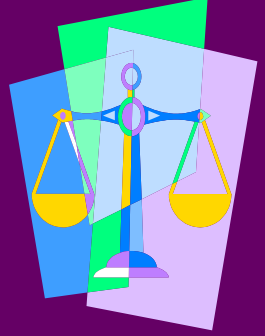
Two Key Privacy Rule Goals

- Provide strong Federal protections for privacy rights
- Preserve quality health care



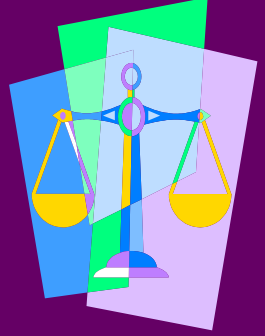
HHS Secretary Thompson August 14, 2002

The Privacy Rule "*strikes a common sense balance by providing consumers with personal privacy protections and access to high quality health care.*"



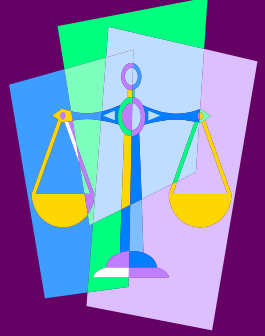
As Modified, Privacy Rule is:

- Flexible and Scalable
- Workable
- Balanced



Today: Key Elements of Privacy Rule

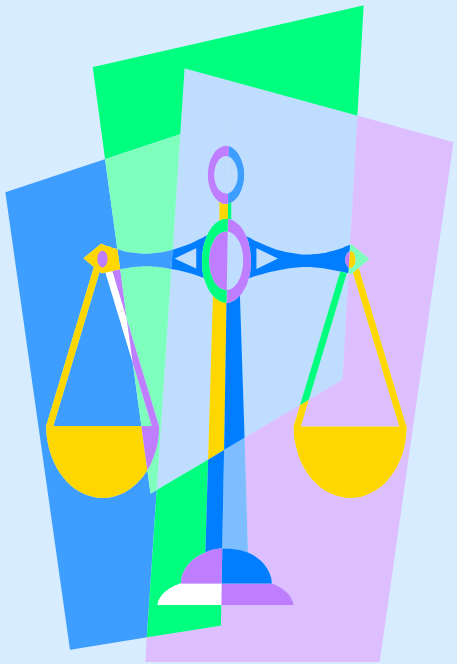
- Covered Entity
- Uses and Disclosures
- Research
- Individual Rights
- Administrative Requirements
- Compliance and Enforcement



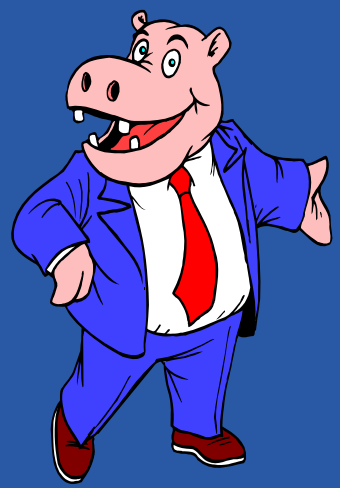
Key HIPAA Dates

Date	Deadline
Oct. 16, 2002	Electronic Health Care Transactions and Code Sets - all covered entities except those who filed for an extension and those that are small health plans
April 14, 2003	**Privacy - all covered entities except small health plans**
April 16, 2003	Electronic Health Care Transactions and Code Sets - all covered entities must have started software and systems testing
October 16, 2003	Electronic Health Care Transactions and Code Sets - all covered entities who filed for an extension and small health plans
April 14, 2004	**Privacy - small health plans**

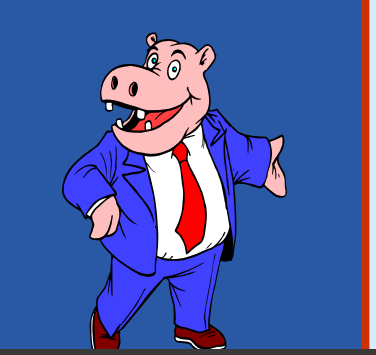
45 CFR § 162.100, 900, § 164.534, P.L. 107-105



Entities Covered by the HIPAA Privacy Rule



United States Department of Health & Human Services

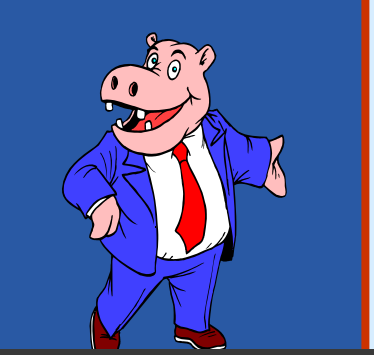


Who Is A Covered Entity?

HIPAA standards apply only to:

- Health care providers who transmit any health information electronically in connection with certain transactions
- Health plans
- Health care clearinghouses

45 CFR §§ 160.102, 164.500



What is a Health Care Provider?

A health care provider is –

- Any person or organization who furnishes, bills, or is paid for health care in the normal course of business

45 CFR § 160.103

Are All Health Care Providers Covered?

Health care providers are covered only if they transmit health information electronically in connection with a transaction covered by the HIPAA Transaction Rule

* Directly or through a business associate

45 CFR § 160.102

HIPAA Transactions Rule Standards

1. Health care claims or equivalent encounter information
2. Health care payment and remittance advice
3. Coordination of benefits
4. Health care claim status
5. Enrollment or disenrollment in a health plan
6. Eligibility for a health plan
7. Health plan premium payments
8. Referral certification and authorization

45 CFR § § 162.1101 – 162.1802

What Is A Health Plan?

Any individual or group plan (or combination) that provides, or pays for the cost, of medical care. Examples include:

- Health insurance issuers
- HMOs
- Group Health Plans
- Medicare, Parts A and B
- Medicare + Choice
- Medicaid

45 CFR § 160.103

What Health Plans Are Covered?

- All health plans are covered
- Entities that are not considered health plans include:
  - Employer plans with fewer than 50 participants and which are self-administered
  - Excepted Benefit Plans
  - Certain government funded programs

45 CFR § 160.103

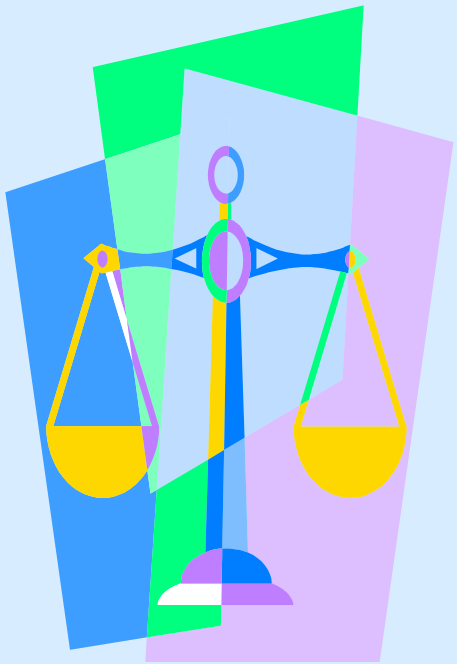
Group Health Plans as Covered Entities

- Under ERISA, a group health plan is a separate legal entity from the employer/plan sponsor
- The Privacy Rule does not cover employers or plan sponsors

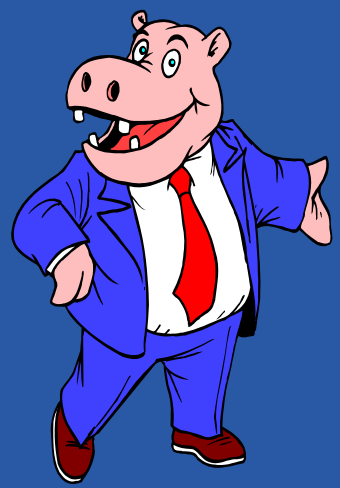
What Is A Health Care Clearinghouse? How does Rule Apply?

- Translates data content or format for another entity from non-standard to standard or vice versa
- Limitation on Applicability of Privacy Rule

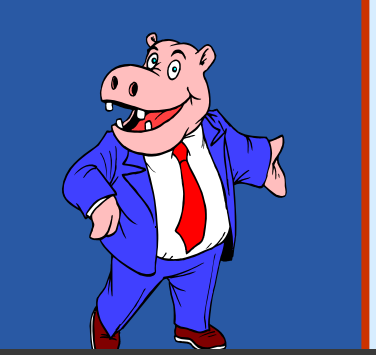
45 CFR § § 160.103, 164.500(b)



Business Associates



United States Department of Health & Human Services



Who Is A Business Associate?

A person who performs a function or activity on behalf of, or provides services to, a Covered Entity that involves Individually Identifiable Health Information

- Is not a workforce member
- Covered Entity can be a Business Associate

45 CFR § 160.103

Examples Outside BA Definition

- Two Covered Entities – each performing functions on its own behalf
  - Provider gives PHI to payer for payment
  - Hospital and physician treating patients at hospital
- Persons or organizations where access to protected health information is not necessary to do their job
  - Janitors, electricians, copy machine repair persons

45 CFR § 160.103

Requirements on Covered Entity

- Obtain “satisfactory assurance” that Business Associate will appropriately safeguard Protected Health Information
  - Written contract or other written arrangement or agreement
- No monitoring
- Cure or terminate contract if known violation

45 CFR §§ 164.502(e), 164.504(e)

Contracts Must Include:

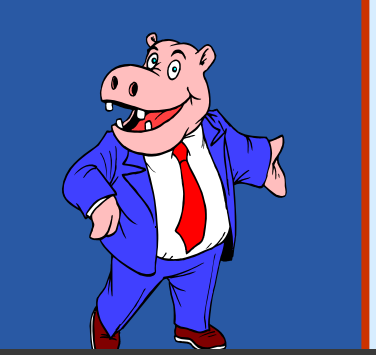
- Permitted uses and disclosures
- Requirement to use appropriate safeguards
- Requirement to report of non-permitted uses and disclosures to Covered Entity
- Requirement to extend same terms to subcontractors/agents

45 CFR § 164.504(e)

Business Associate Exceptions

- Disclosures to a provider for treatment to an individual
- Disclosures by a group health plan to plan sponsor if for plan administration
- Uses or disclosures by a government health plan (e.g., Medicare) to another agency (e.g., SSA) for eligibility or enrollment determinations if authorized by law

45 CFR § 164.502(e)

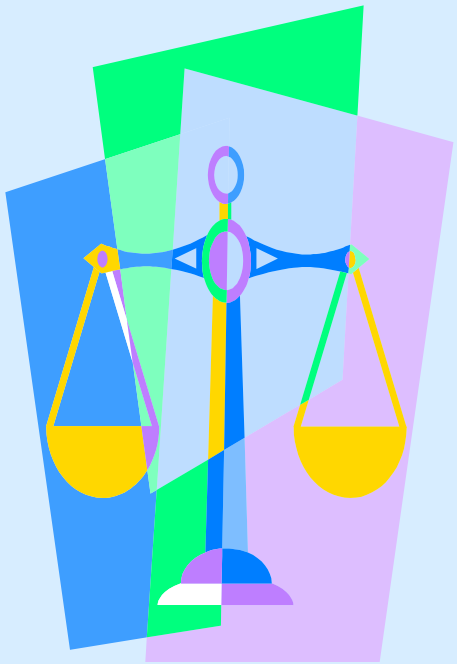


Transition Provisions

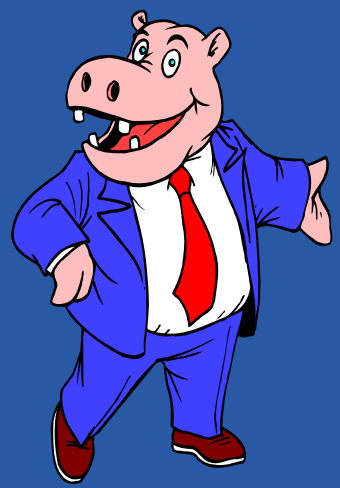
For a written contract existing as of 10/15/02 and not renewed or modified by 4/14/03:

- Covered Entities are allowed until 4/14/04 to have contract comply with Privacy Rule requirements

45 CFR § 164.532(d)



Group Health Plan Disclosures to Plan Sponsors



United States Department of Health & Human Services

Types of Disclosures to Plan Sponsors

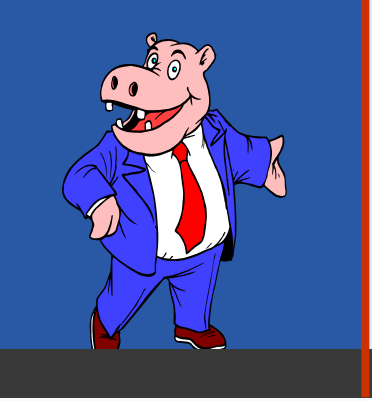
- Summary health information; Enrollment and disenrollment information
- Amend plan documents
- With individual authorization

45 CFR § § 164.504 (f), (a), 164.508

Summary Health Information, Enrollment & Disenrollment

- May disclose summary health information for:
  - Obtaining premium bids from health plans
  - Modifying, amending or terminating health plans
- Enrollment or disenrollment in a health plan

45 CFR § 164.504(f)

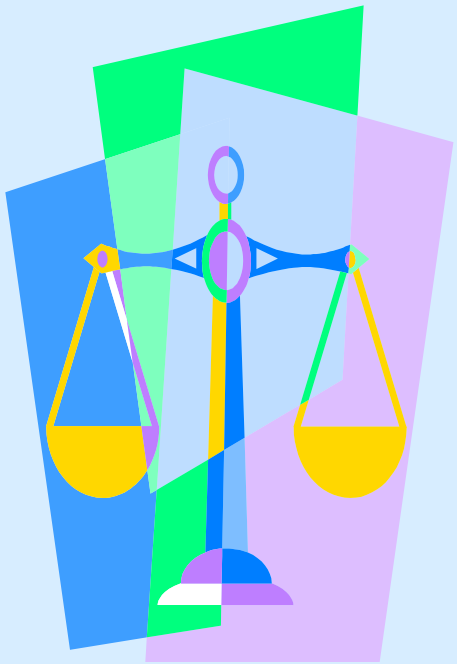


Adequate Assurances from Plan Sponsor

Group health plan may disclose PHI to plan sponsor for plan administrative functions if:

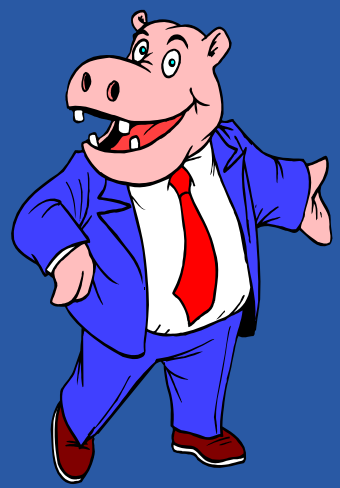
- plan documents are amended to provide permitted and required uses/disclosures by plan sponsor
- Certification by plan sponsor
- Adequate separation (“erect firewalls”)

45 CFR § 164.504(f)

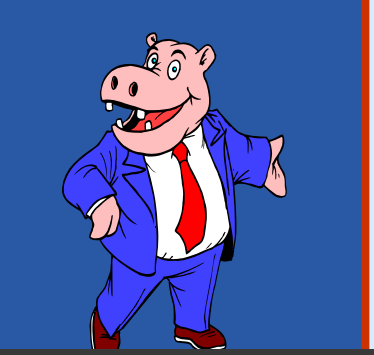


ORGANIZATIONAL ISSUES

- Hybrid Entities
- Affiliated Covered Entities
- Organized Health Care Arrangements



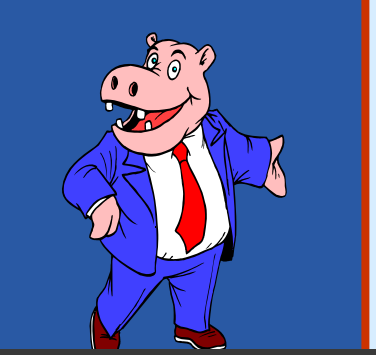
United States Department of Health & Human Services



Choosing Hybrid Entity Status

- Covered Entity that does both covered and non-covered functions
- Option to restrict the application of the Privacy Rule to certain parts of its organization
- By designating health care components (HCC)
- This designation will make the Covered Entity a “Hybrid Entity” under the Rule

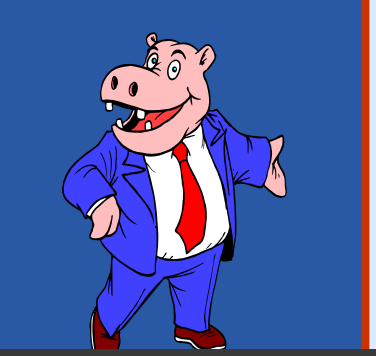
45 CFR § § 164.103, 105



Effects of Hybrid Status

Covered Entity retains administrative and legal responsibilities

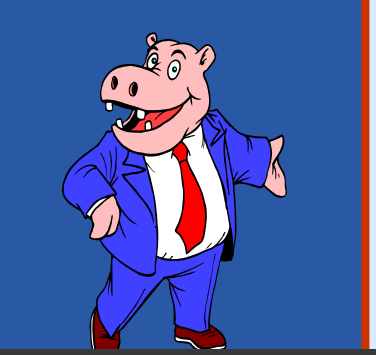
- Must ensure that –
  - **The Health Care Component complies with Privacy Rule (“erect firewalls”)**
  - **Workforce members who perform tasks for both the HCC and non-HCC do not inappropriately use or disclose PHI**
- Has legal responsibility for complying with Privacy Rule



Affiliated Covered Entity

- Legally separate Covered Entities
- Under common ownership or control
- Option to be treated as a single legal entity
- By choosing to designate
- This designation will make the Covered Entity an “Affiliated Covered Entity” under the Rule

45 CFR § § 164.103, 164.105(b)



Effects of Affiliated Covered Entity Status

- May be able to share information in a way that would otherwise be impermissible (sharing becomes a “use” not a “disclosure”).
- May minimize administrative burdens
- BUT, each is separately subject to liability for enforcement actions, and could be cumbersome to devise and comply with uniform set of policies, and/or one notice

45 CFR § 164.105(b)

Organized Health Care Arrangement (OHCA)

Several defined arrangements are OHCAs:

- **Clinically integrated care settings (e.g., hospital and doctors on medical staff)**
- **Covered entities that hold themselves out to the public as participating in joint arrangements and engage in certain joint activities (e.g., IPA)**
- **Certain group health plan arrangements**

45 CFR § 160.103

OHCA: Application of the Rule

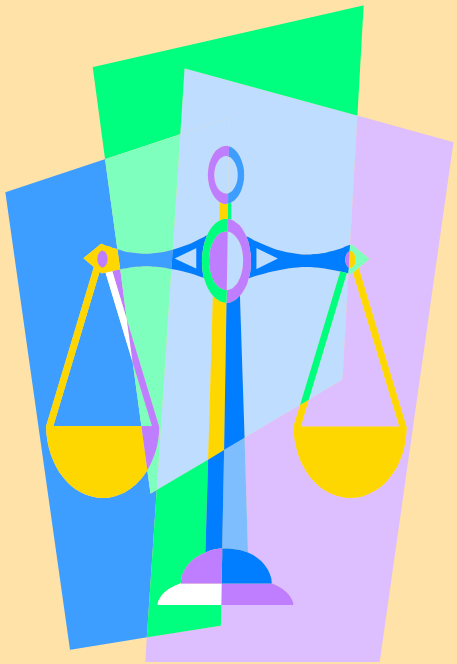
- OHCA or its members can choose whether or not:
  - To contract as one entity with a business associate
  - To disclose PHI to another covered entity that participates in the OHCA for joint health care activities of the OHCA
  - To have joint notices – only need be provided once
- BUT, each is separately subject to liability for enforcement actions

45 CFR § § 160.103, 164.520(d)

Summary

Rule applies to:

- Providers that conduct certain transactions electronically
- Health plans
- Clearinghouses



Protected Health Information

United States Department of Health & Human Services

What Is Covered?

- Protected health information (PHI)
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium by a Covered Entity or its Business Associate

45 CFR § 160.103

Individually Identifiable Health Information

- Health information, including demographic information
- Relates to an individual's physical or mental health or the provision of or payment for health care
- Identifies the individual

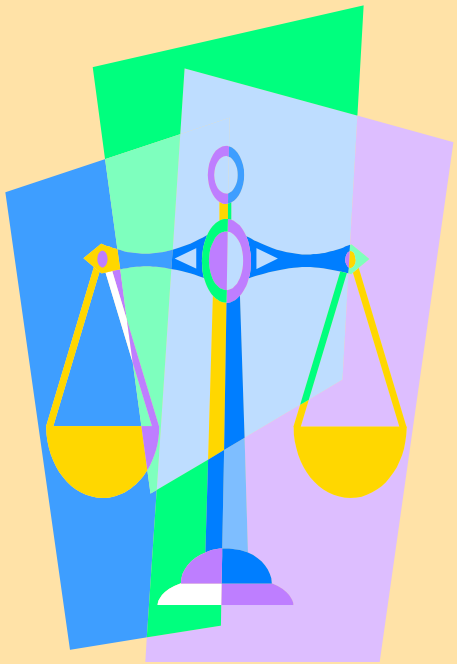
What is NOT Covered?

Not PHI:

- Employment records of Covered Entity
- Family Educational Rights and Privacy Act (FERPA) records

De-identification of PHI

- Removal of certain identifiers so that the individual who is subject of the PHI may no longer be identified
- Application of statistical method or
- Stripping of listed identifiers such as:
  - Names
  - Geographic subdivisions < state
  - All elements of dates
  - SSNs



Uses & Disclosures of PHI

United States Department of Health & Human Services

General Rule

Covered Entity may not use or disclose PHI, except as permitted or required by Privacy Rule

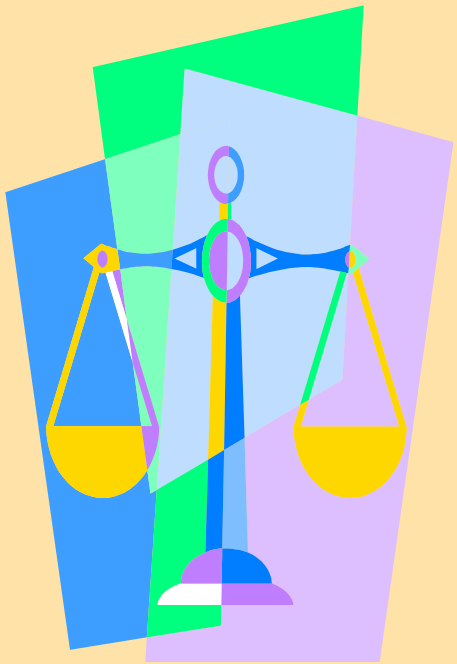
Required Disclosures

- To individual when requested & required by Section 164.524 (Access) & Section 164.528 (Accounting)
- To HHS, to investigate or determine compliance with Privacy Rule

Permitted Uses and Disclosures

- Individual
- Treatment, Payment and Health Care Operations (TPO)
- Opportunity to Agree or Object
- Public policy
- "Incident to"
- Limited data set
- Authorized

45 CFR § 164.502(a)



To the Individual

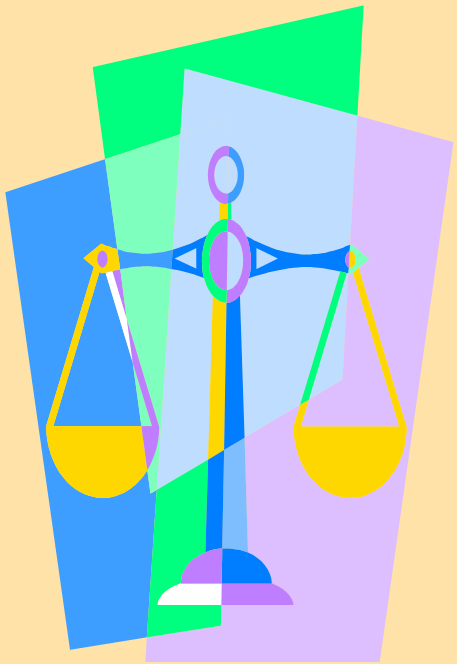
United States Department of Health & Human Services

To Individuals

Besides required disclosures, Covered Entities also may disclose PHI to their patients/health plan enrollees
Examples:

- Health plans can contact their enrollees
- Providers can talk to their patients

45 CFR § 164.502(a)



Treatment, Payment and Health Care Operations

United States Department of Health & Human Services

Treatment, Payment and Health Care Operations (TPO)

Covered Entity may use/disclose PHI to carry out essential health care functions

- Treatment
- Payment
- Health care operations

45 CFR § § 164.502(a), 164.506

Treatment

Treatment means the provision, coordination, or management of health care by one or more health care providers, including:

- consultation between health care providers; or
- patient referrals

Payment

- Payment means activities of:
- Health care providers to obtain payment or be reimbursed for their services
- Health plans to obtain premiums, fulfill coverage responsibilities, or provide reimbursement for the provision of health care

Health Care Operations (1)

- Health Care Operations are administrative, financial, legal and quality improvement activities
- Necessary to run business and to support core functions of treatment and payment

Health Care Operations (2)

- Quality assessment and improvement activities
- Training, accreditation, certification, credentialing, licensing, reviewing competence, evaluating performance
- Fraud and abuse detection

Health Care Operations (3)

- Underwriting, rating, other activities relating to the creation, renewal or replacement of a contract of health insurance or benefits
- Conducting or arranging for medical review, legal services, or auditing
- Business planning and development
- Business management and general administrative activities

45 CFR § 164.501

Sharing for TPO (1)

- Use/disclose PHI for own TPO
- Disclose for treatment activities of a provider
- Disclose to another Covered Entity or provider for recipient's payment activities

45 CFR § 164.506(c)

Sharing for TPO (2)

- Disclose to another Covered Entity, if mutual relationship with individual, for other Covered Entity's
  - quality, training/credentialing
  - fraud and abuse detection activities
- Disclose to another OHCA member for their joint health care activities

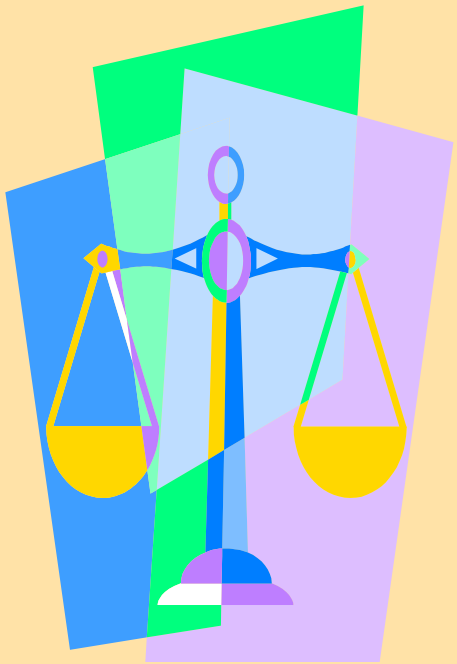
45 CFR § 164.506(c)

Optional Consent

Rule permits consent on voluntary basis for TPO

- Optional consent may not be used where an authorization is required

45 CFR § 164.506(b)



Opportunity for Individual to Agree or Object

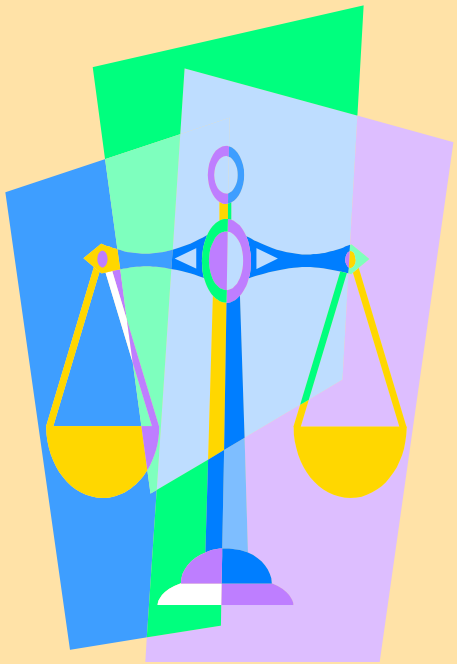
United States Department of Health & Human Services

Facility Directories

- Must give individual opportunity to restrict or prohibit (can be oral) the use or disclosure of name, location, general condition, and religious affiliation for:
  - Disclosure to persons who request the individual by name (except religion)
  - Disclosure to clergy
- Emergency exception

Family, Friends, and Advocates

- Must give individual opportunity to agree or object:
  - **May disclose PHI relevant to person's involvement in care or payment** to family, friends, or others identified by individual
  - **May notify of individual's location, condition, or death** to family, personal representatives, or another responsible for care
    - Applies to disaster relief efforts
- When individual is not present or incapacitated:
  - Above uses and disclosures are permissible using professional judgment to determine if in best interest of individual



Public Policy Uses and Disclosures

United States Department of Health & Human Services

Public Policy Purposes

(a) As required by law

(b) For public health

(c) About victims of abuse, neglect or domestic violence

(d) For health oversight activities

(e) For judicial & administrative proceedings

(f) For law enforcement purposes

45 CFR § 164.512(a)-(f)

Public Policy Purposes (2)

(g) About decedents (to coroners, medical examiners, funeral directors)

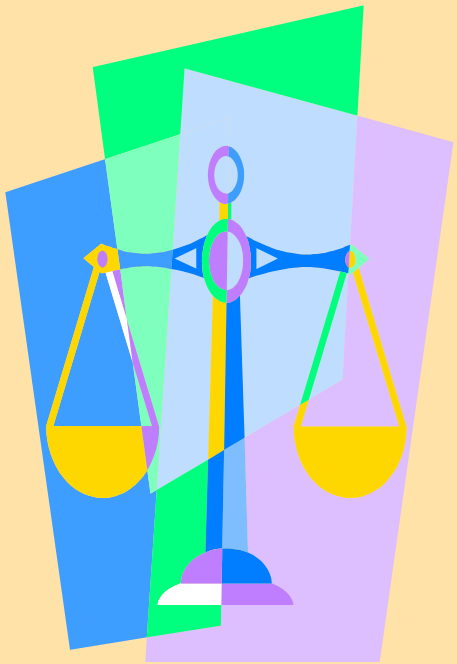
(h) For cadaveric organ, eye or tissue donations

(i) For research purposes

(j) To avert a serious threat to health or safety

(k) For specialized government functions (military, veterans, national security, protective services, State Dept., correctional

(l) For workers' compensation

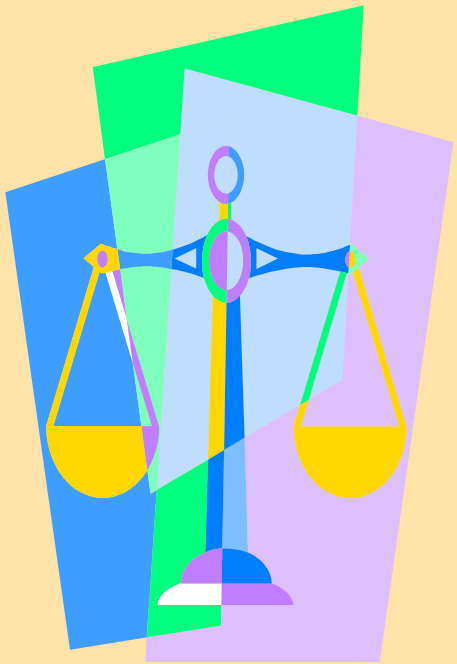


Overheard, Seen in Passing…

United States Department of Health & Human Services

“Incident to” Uses and Disclosures

- Rule permits uses/disclosures incident to an otherwise permitted use or disclosure, provided minimum necessary & safeguards standards are met
- Allows for common practices if reasonably performed



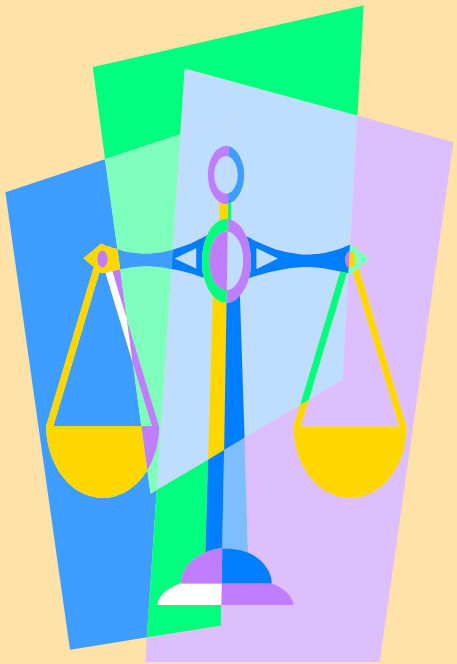
Limited Data Set

United States Department of Health & Human Services

Limited Data Set

- For research, public health, health care operations purposes
- Direct identifiers must be removed
- Allows zip codes, dates
- Requires Data Use Agreement: recipient cannot use for other purposes or identify or contact individuals

45 CFR § 164.514 (e)



Authorized Uses and Disclosures

United States Department of Health & Human Services

Uses/Disclosures Requiring Authorization

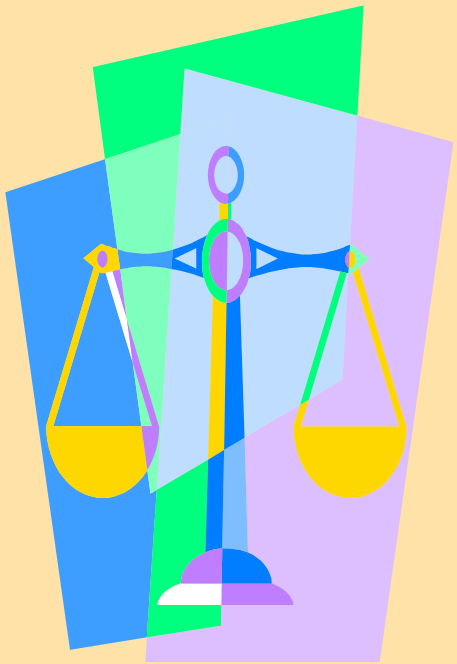
Authorizations are required for uses and disclosures not otherwise permitted or required by the Rule

45 CFR § 164.508(a)

Authorization

- Generally, cannot condition treatment, payment, eligibility, or enrollment on an authorization
- Special rules:
  - psychotherapy notes
  - marketing
- Authorization must contain core elements & required statements, including:
  - Expiration Date or event
  - Statement that authorization is revocable

45 CFR § 164.508(a)-(c)



Minimum Necessary

United States Department of Health & Human Services

Minimum Necessary

Covered entities must make reasonable efforts to limit the use or disclosure of, and requests for, PHI to minimum amount necessary to accomplish intended purpose

Policies & Procedures for Uses, Disclosures, Requests

- **Uses**
  - Role-based access
- **Disclosures & Requests**
  - Standard protocols for routine/recurring
  - Case-by-case review for non-routine

Reasonable Reliance

Covered entities may reasonably rely upon requester's determination as to minimum amount necessary if:

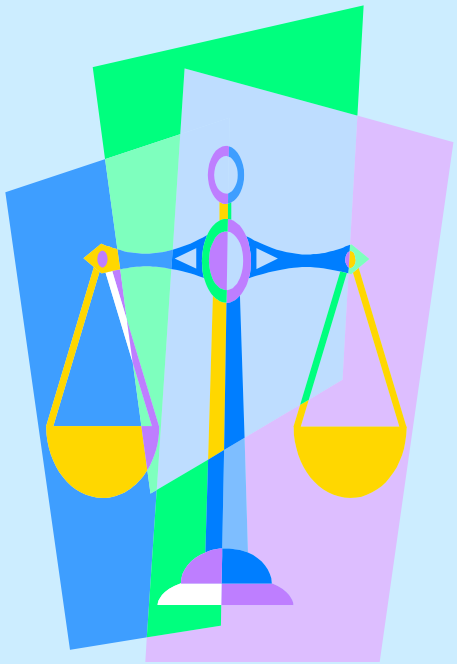
- Public official
- Another covered entity
- Business associate for provision of professional service
- Researcher with IRB/Privacy Board documentation or other appropriate representations

Minimum Necessary Exceptions

- Disclosures to or requests by providers for treatment
- Disclosures to individual
- Uses/disclosures with an authorization
- Uses/disclosures required for HIPAA standard transaction
- Disclosures to HHS/OCR for enforcement
- Uses/disclosures required by law

Summary

- What information is covered under the Privacy Rule
- What Covered Entities can do with that information
- How much information can flow, and to whom in the organization



Research

United States Department of Health & Human Services

Research Provisions

- Covered entities may use and disclose PHI for research:
  - with individual authorization, or
  - without individual authorization under limited circumstances

45 CFR § § 164.508, 164.512(i)

What Research is Affected?

- Records research that uses existing PHI, such as:
  - Research databases and repositories
- Research that includes treatment of research participants, such as
  - Clinical trials

Relationship to Other Research Rules

The Privacy Rule **does not** override the Common Rule or FDA's human subject protection regulations

Common Rule vs. Privacy Rule

***Research <u>WITH</u>* patient permission**

Common Rule/FDA Regulated

↓

IRB review of research and informed consent

Privacy Rule

↓

Valid authorization

Privacy Authorization

- Research participant authorization to use or disclose PHI is required for most clinical trials and some records research
  - May be no expiration date or event or may continue until “end of research study”
  - May be combined with informed consent to participate in research

45 CFR § 164.508(c), (b)

Common Rule vs. Privacy Rule

*Research **WITHOUT*** patient permission

Common Rule

- IRB Review—
  4 waiver criteria

Privacy Rule

- IRB/Privacy Board Review—
  3 waiver criteria
- Preparatory research;
- Research on decedents; or
- Limited data set

45 CFR § § 164.512(i), 164.514(e)

Use and Disclosure of PHI for Research *Without* Individual Authorization:

Four Options:

- **OPTION 1:** Obtain documentation that an IRB or Privacy Board has approved an alteration to or waiver of authorization based on the following 3 waiver criteria:

3 Waiver Criteria

1) The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements…

Minimal Risk Elements

a. an adequate plan to protect the identifiers from improper use/disclosure;

b. an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining identifiers or such retention is otherwise required by law; and

c. adequate written assurances that PHI will not be reused/disclosed to any other person or entity, with certain exceptions.

Waiver criteria…

2) The research could not practicably be conducted without the alteration or waiver

3) The research could not practicably be conducted without access to and use of the PHI

Research Use and Disclosure of PHI *Without* Individual Authorization:

- **OPTION 2:** Obtain representation that the use or disclosure is necessary to prepare a research protocol or for similar purposes preparatory to research
  - No PHI removed from Covered Entity

Research Use and Disclosure of PHI *Without* Individual Authorization:

- **OPTION 3:** Obtain representation that the use or disclosure is solely for research on decedents' protected health information

Research Use and Disclosure of PHI *Without* Individual Authorization

- **OPTION 4:** Only use or disclose limited data set/"indirect identifiers" (e.g. zip codes, dates of service, age, death)
  - Requires a data use agreement

Accounting for Research Disclosures

- Upon request, must provide accounting for research disclosures made without individual authorization (except for disclosures of the limited data set).
- For 50+ records:
  - List of protocols for which PHI may have been disclosed, and
  - Researcher contact information

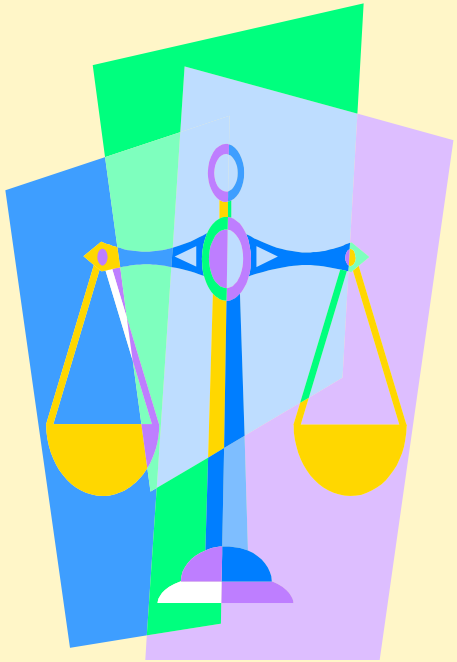
45 CFR § 164.528(a), (b)

Covered Entity and Researcher Relationship

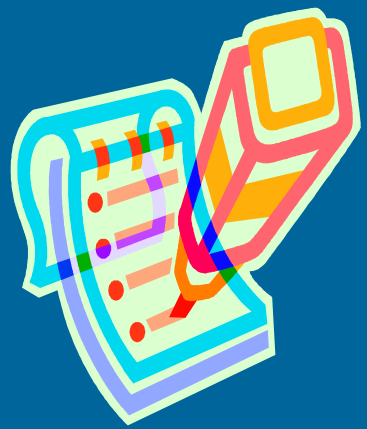
- Researcher within Covered Entity
  - Rule applies to entire entity; or
  - Elect Hybrid status
    - Must include clinical researcher in covered component if covered health care provider
    - May include clinical researcher in covered component even if not covered health care provider
    - May not include researcher that is not also providing health care
- Researcher and Covered Entity are two separate legal entities

Ongoing Research at Time of Compliance Date (4/14/03)

- Grandfathers in use or disclosure of PHI as permitted by the following if obtained prior to the compliance date:
  - Legal permission for the use or disclosure PHI;
  - Informed consent for the research; or
  - An IRB waiver of informed consent under the Common Rule.



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

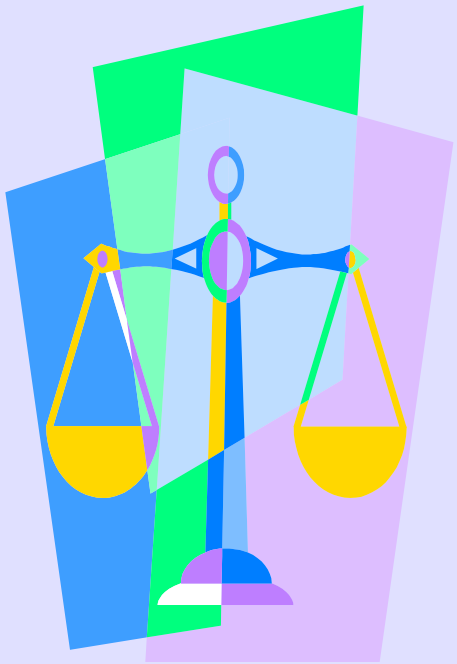
45 CFR §164.530(k)

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

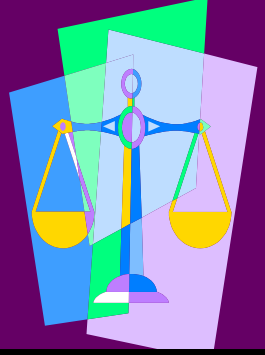
Common Compliance Issues to Consider

- 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



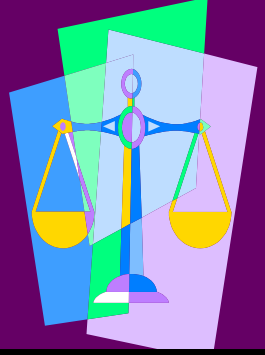
Compliance and Enforcement of the Privacy Rule

United States Department of Health & Human Services



Compliance Date

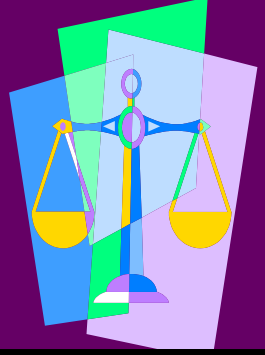
- April 14, 2003 – Compliance for all but small health plans
- One year extension for small health plans
- No statutory extension available in Privacy Rule, unlike extension available for Transaction Rule through 10/16/03



Office for Civil Rights

- Enforces Civil Rights laws and the Privacy Rule
- With respect to the Privacy Rule:
  - Promote voluntary compliance
  - Investigation and Resolution of Complaints
  - Exception Determinations

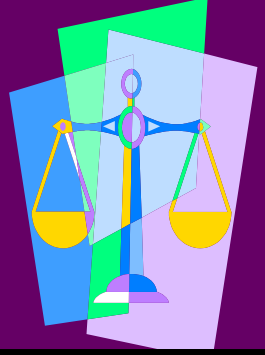
See, e.g.65 Fed. Reg. 82472 (Dec. 28, 2000); 68 Fed. Reg. 13711 (Mar. 20, 2003)



Why Voluntary Compliance?

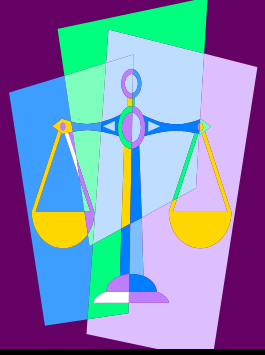
- Promoted by HIPAA statute and Privacy Rule
  - Education, Cooperation, Technical Assistance
  - Permitted even after investigation commences
  - Can help mitigate CMPs
- Most efficient way to promote privacy

42 USC §1320d-5, §160.304



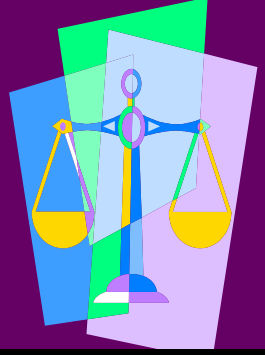
Technical Assistance

- Integrated Rule and Preambles to Dec. 2000, Aug. 2002 Final Rules
- Covered Entity decision tool
- December 4, 2002 Guidance
- Targeted Technical Assistance materials under development
- Fact sheet on August 2002 modifications
- Sample Business Associate Contract
- FAQs on our website
- http://www.hhs.gov/ocr/hipaa/



December 4, 2002 Guidance

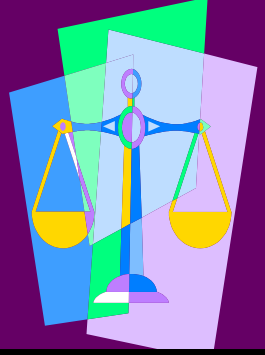
- General Overview
- Incidental Uses and Disclosures
- Minimum Necessary
- Personal Representatives
- Business Associates
- Uses and Disclosures for Treatment, Payment and Health Care Operations
- Marketing
- Public Health
- Research
- Workers' Compensation Laws
- Notice
- Government Access
- Miscellaneous FAQs



Investigations & Compliance Reviews

- OCR may investigate complaints
- OCR may conduct compliance reviews to determine whether Covered Entities are in compliance

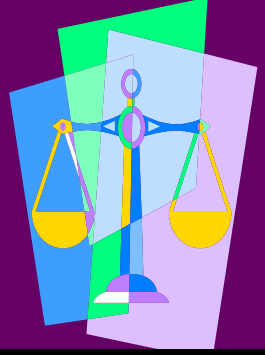
45 CFR § § 160.306, 160.308



Filing Complaints

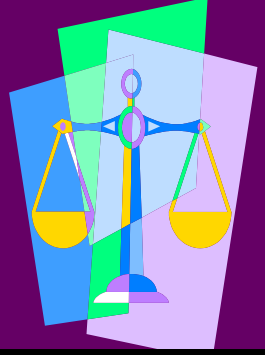
- Any person or organization may file complaint with OCR by mail or electronically
  - Only for possible violations occurring after compliance date
  - Complaints should be filed within 180 days of when the complainant knew or should have known that the act or omission occurred
- Individuals may also file complaints with Covered Entity

§160.306, 68 Fed. Reg. 13711 (Mar. 20, 2003)



Complaint Process

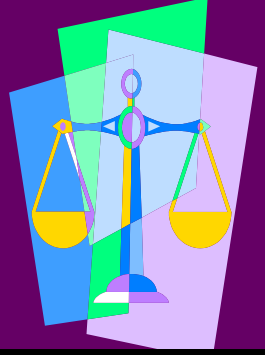
- Informal review may resolve issue fully without formal investigation
  - Many complaints will be resolved at this stage
- If not, begin investigation
  - Voluntary resolution yet possible
- Technical Assistance



Civil Monetary Penalties (CMPs)

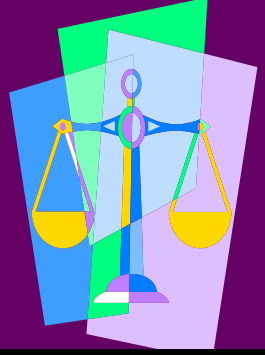
- CMPs can be imposed by OCR:
  - $100 per violation
  - Capped at $25,000 for each calendar year for each identical requirement or prohibition that is violated
    - Covered Entity has a right to notice and a hearing before a CMP becomes final

42 USC §1320d-5



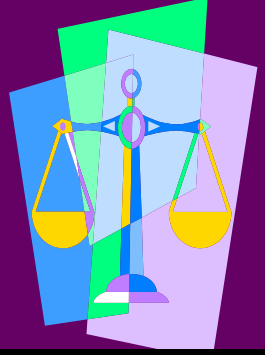
No CMPs if:

- Person did not know – and by exercising reasonable diligence would not have known - of the violation
- If failure to comply is due to reasonable cause and not willful neglect and entity corrects within 30 day cure period
- Offense is punishable by criminal sanction



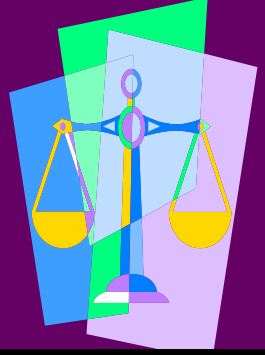
CMP Flexibility Summary

- Exceptions
- Potential extension of the 30 day cure period
- CMP reduction possible if:
  - Amount excessive relative to violation
  - Due to reasonable cause/not willful neglect



Criminal Penalties for Wrongful Disclosures

- For knowingly obtaining or disclosing identifiable health information relating to an individual in violation of the Rule:
  - Up to $50,000 & 1 year imprisonment
  - Up to $100,000 & 5 years if done under false pretenses
  - Up to $250,000 & 10 years if intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm
- Enforced by DOJ



Additional Information

www.hhs.gov/ocr/hipaa/

OCR Privacy Toll Free Number: (866) 627-7748