HIPAA's Medical Privacy Standards:

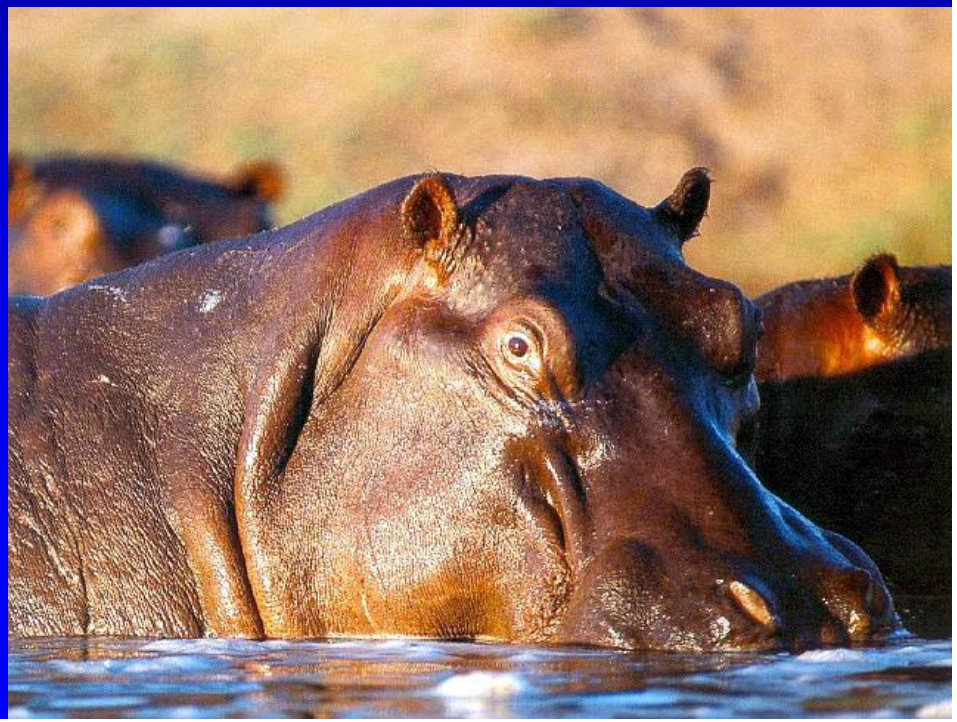
The Long and *Really* Winding Road

Michael D. Bell, Esq.
Mintz, Levin, Cohn, Ferris,
Glovsky and Popeo, P.C.
Washington, D.C.
(202) 434-7481
mbell@mintz.com

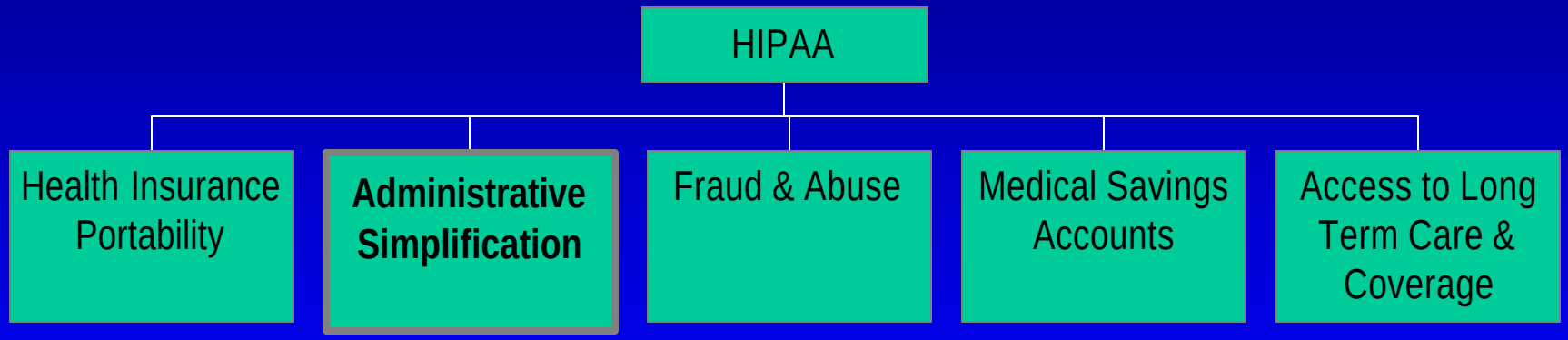
MINTZ LEVIN
COHN FERRIS
GLOVSKY AND
POPEO PC

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)

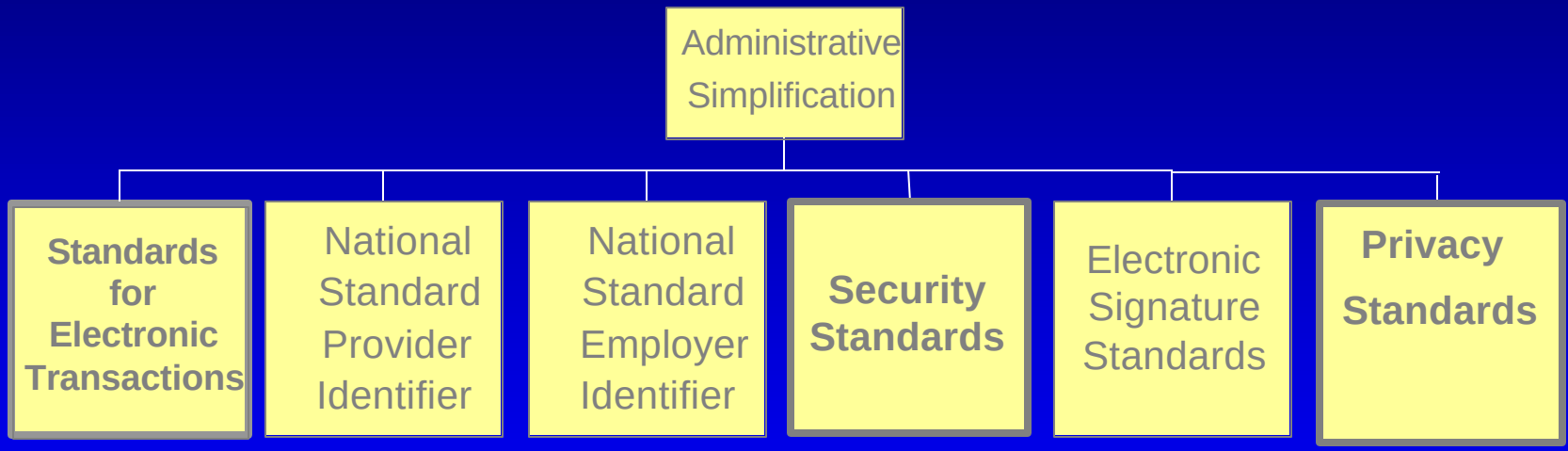
The Road to Privacy



The Multiple Components of HIPAA



Components of “Administrative Simplification”



Standards for Electronic Transactions

Standards, Transactions and Code Sets

- In December 2001, Congress extended the deadline for the transaction set rule
- New deadline is October 16, 2003
- Entities that want an extension must submit a detailed plan for compliance to HHS
- No effect on deadline for Privacy Regulation

ASCA

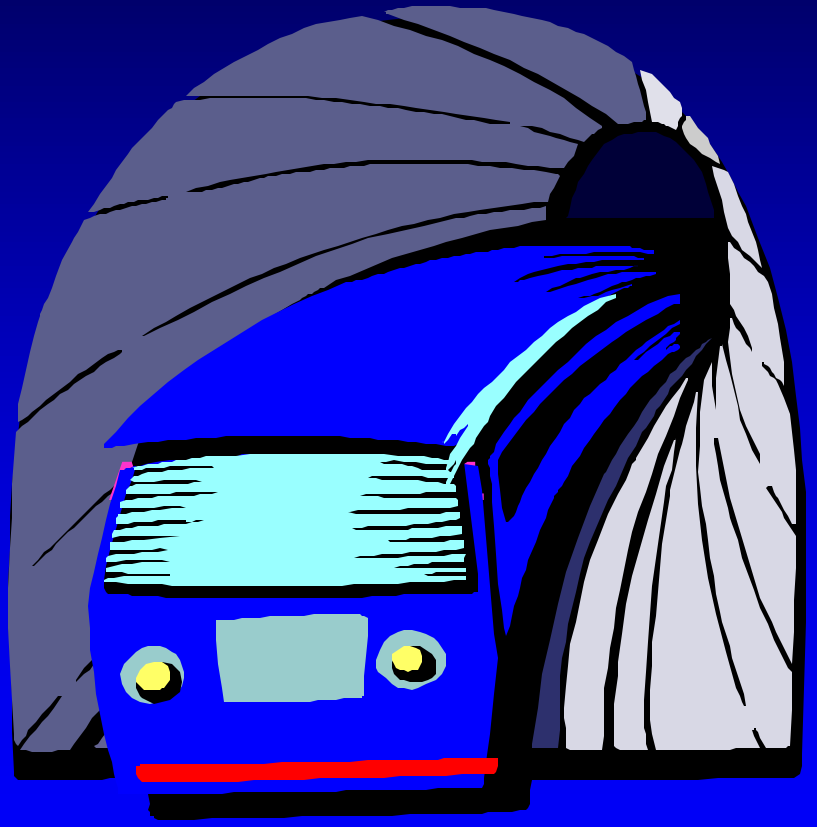
- On December 27, 2001, President Bush signed into law the Administrative Simplification Compliance Act.
- By October 16, 2002, covered entities must either:
  - be in compliance with the Standards for Electronic Transactions and Code Sets; or
  - submit a summary plan to the Secretary of Health and Human Services describing how the covered entity will come into full compliance with the standards by October 16, 2003.
- No effect on deadline for Privacy Regulation

ASCA

- HHS recently issued a model form that covered entities must complete in order to obtain the one-year compliance extension
- “Multiple related covered entities that are operating under a single implementation plan” are permitted to submit one form
- Forms are due by 10-15-02
- http://www.cms.hhs.gov/hipaa/hipaa2/ASCAForm.asp

Privacy Regulation

- Final regulation became effective April 14, 2001, and providers have 2 years from that date to be in compliance
- HHS issued its first set of implementation guidance in July 2001
- Major revision issued March 27, 2002, 67 Fed. Reg. 14776



Privacy Regulation GOALS

- Give consumers control over their health information
- Regulate the use, disclosure and receipt of an individuals' health information
- Ensure security of personal health information
- Establish accountability for health information use and release

Privacy Regulation COMPLIANCE DATE

- Covered entities must be in compliance with the rule by April 14, 2003
- March 2002 Proposal would extend Business Associate requirements for a year, under certain circumstances

March 2002 Proposed Changes

- In March 2002 HHS issued proposed changes to the Privacy Regulation
- Extensive and far-reaching changes
- Generally well-received by the health care community
- Comments due by April 26th
- Does not affect compliance date

March 2002 Proposed Changes

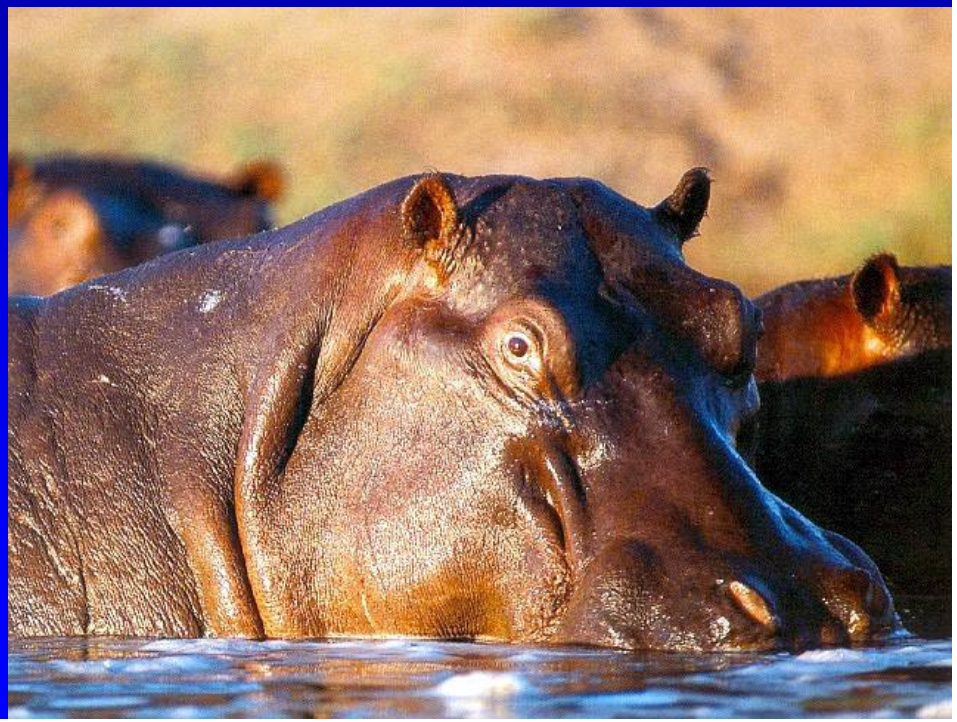
- Consent becomes optional
- Good faith effort to obtain acknowledgement of Notice of Privacy Practices
- Simplifies Minimum Necessary requirements
- Delays compliance of Business Associate contracts, until modification or renewal

March 2002 Proposed Changes

- Simplifies marketing requirements
- Eases restrictions on research uses
- Greater rights to parents with respect to their children
- New standards for de-identification

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)

Scope of the Privacy Regulation



“In a Nutshell”

- The Privacy Regulations govern a covered entity’s use and disclosure of protected health information and grant individuals certain rights with respect to their protected health information.
- HIPAA sets the “floor” not the “ceiling”—more stringent state laws are not preempted.

Who is covered?

- Covered entities
  - health plans;
  - health care clearinghouses; and
  - providers that transmit health information in electronic form in connection with a HIPAA standardized transaction
- Also reaches the “Business Associates” of the covered entity

Organizational Structures

- A "**hybrid entity**" means a single legal entity that performs both covered and non-covered functions.
- **Affiliated Covered Entities**--the rules permit legally distinct covered entities that share common ownership or control to designate themselves, or their health care components, together to be a single covered entity
- **Organized health care arrangements** are arrangements involving clinical and/or operational integration among legally separate covered entities

Hybrid Entity March 2002 Proposed Changes

- In the March 2002 Proposal, HHS eliminates the “primary purpose” requirement, permitting any covered entity whose business activities include both covered and non-covered functions to designate itself as a hybrid entity.

Protected Health Information (PHI)

All individually identifiable health information that is transmitted or maintained in any form or medium.

Individually Identifiable Health Information

- Created or received by a covered entity or employer; and
- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual and which:
  - Identifies the individual; or
  - Offers a reasonable basis for identification of the individual

De-Identification

- PHI does not include information that has been “de-identified”:
  - specified list of identifiers removed; or
  - determination by statistical expert that risk of identification is very small
- Covered entity may assign code or other means of record identification to allow de-identified information to be re-identified if:
  - code not derived from or related to information otherwise capable of identifying the individual; and
  - covered entity does not use/disclose the code for any other purpose or disclose the mechanism for re-identification

De-Identification March 2002 Proposed Changes

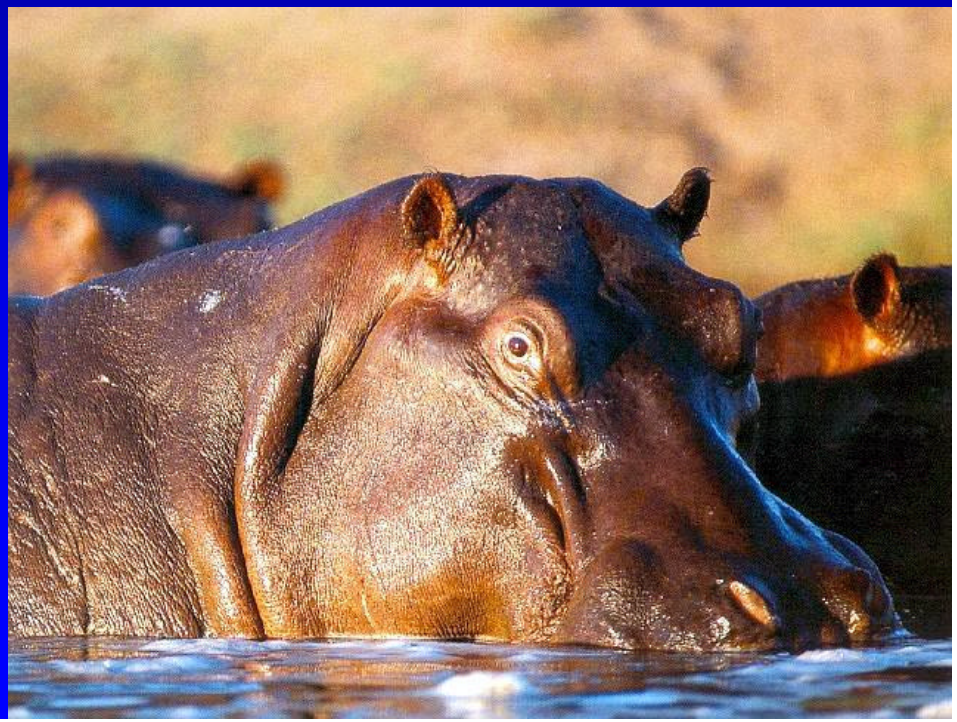
- March 2002 Proposal requests comment on an alternative approach to de-identification
- Permits disclosure of limited data set that includes certain identifiers
- Disclosure only for research, public health, and health care operations
- Recipients of data would have to agree to limit its use

De-Identification March 2002 Proposed Changes

- Limited Data Set
  - Admission, discharge and service dates
  - Date of death
  - Age
  - Five digit zip code

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)

Key Concepts



Uses and Disclosures of PHI

- 4 types of "Permissions"
  - Consent
  - Oral agreement
  - None required
  - Authorization

Consent

- Direct health care providers must obtain consent from an individual before using or disclosing PHI for treatment, payment, or health care operations
- Once a consent is obtained, it may be used forever unless it is revoked in writing by the individual who gave it.
- In most circumstances, if the patient refuses to give consent for TPO, the provider may refuse to treat the patient

Consent Under the March 2002 Proposal

- Consent not required for TPO, although providers have the option of obtaining it
- Providers with a direct treatment relationship are required to make a “good faith effort” to obtain written acknowledgement of receipt of Notice
- Covered entity can disclose PHI to another entity for payment activities and some health care operations of the other entity, without consent

Authorizations

- If not otherwise permitted by the regulation, an authorization must be obtained – e.g., certain marketing activities, research, employment determinations, fund raising, psychotherapy notes
- Must be written in plain language and contain specific elements
- Only valid until the date/event specified, or until it is revoked in writing by the patient

Authorizations Under the March 2002 Proposal

- Requires all authorizations to contain certain core elements
- Where the individual that is the subject of the PHI initiates authorization for his own purposes, he does not have to reveal purpose
- Only marketing authorizations have to disclose any remuneration that may result

Authorizations Under the March 2002 Proposal

- All authorizations must contain statements regarding the following:
  - The right to revoke and process for doing so
  - Treatment, payment, enrollment eligibility for benefits not conditioned on authorization
  - Where “conditioning” is permissible, statement regarding the consequences
  - The potential for re-disclosure by recipient

Research

- "Research" has same definition as in the Common Rule
- Covered entities may use/disclose PHI for research if:
  - Obtain patient authorization;
  - Obtain documentation of an IRB or Privacy Board approval of a waiver of authorization; or
  - Obtain from the researcher representations that the use/disclosure is sought solely to review PHI as necessary to prepare a research protocol, no PHI will be removed from the covered entity in the course of the review, and PHI is necessary for the research purposes

Research Under the March 2002 Proposal

- Criteria for waiver made more consistent with requirements of Common Rule
- Simplify research authorizations:
  - Permit “end of research” or “none” for expiration date
  - Eliminate special authorization for research involving treatment
  - Permits research authorization to be combined with other legal documents related to the research

Minimum Necessary

- When using, disclosing or requesting PHI, a covered entity must limit PHI to the "minimum necessary to accomplish the intended purpose of the use, disclosure or request" except when:
  - Disclosing for purposes of treatment
  - Uses or disclosures made to the individual
  - Disclosures made to HHS
  - Uses or disclosures required by law

Minimum Necessary Under the March 2002 Proposal

- Permits incidental uses and disclosures, so long as reasonable safeguards in place
- Exempts from minimum necessary rule any uses or disclosures where entity has valid authorization
- Makes requirements applicable to requests for PHI more consistent with those applicable to disclosures of PHI

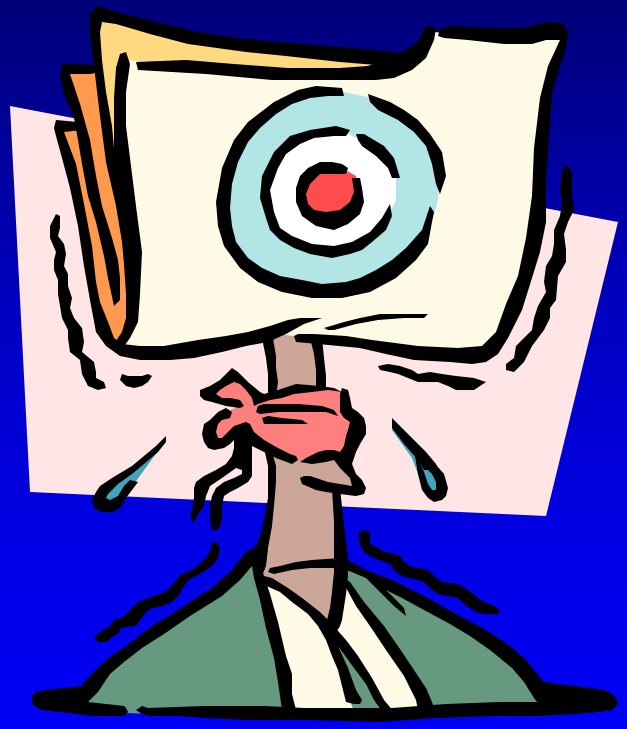
Business Associates

"Business associates" ("BA") are defined as persons, other than workforce members, who perform or assist in the performance of a function on behalf of, or provide services to, a covered entity and such function or service involves the use or disclosure of PHI.

Business Associates

- It is important to note that the BA relationship does not describe all relationships between covered entities and other persons or organizations
- BA contracts are only required where/when:
  - the covered entity is disclosing PHI to someone or some organization that will use the info on behalf of the covered entity
- BA requirements do not apply to covered entities who disclose PHI to providers for treatment purposes (i.e., hospital and physician; laboratory and physician)

Business Associates



If the covered entity becomes aware of a violation of the rule by a business associate and fails to act in response, it can be PENALIZED. The fact that the business associate is performing the functions on behalf of the covered entity DOES NOT insulate the covered entity from enforcement.

Business Associates Under the March 2002 Proposal

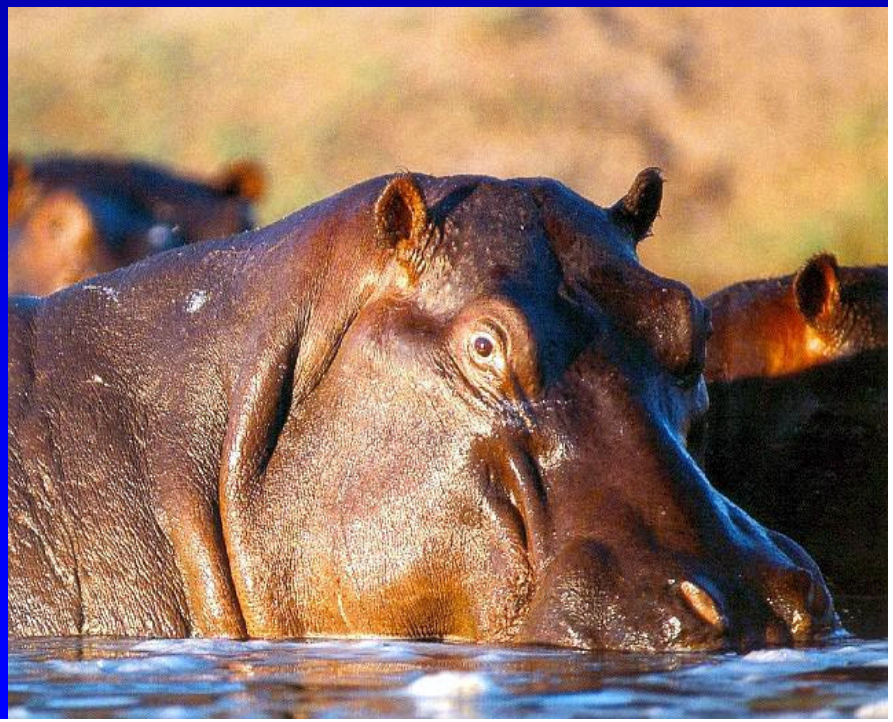
- Existing contracts with BAs will not have to be compliant until April 14, 2004, unless renewed or modified in the interim
- Sample contract language is included in the appendix

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)

Patient Rights

Administrative Requirements

Enforcement



Patient Rights

- Notice of Privacy Practices
- Access, inspect and copy
- Accounting of disclosures
- Request amendments
- Restrict disclosures
- Request privacy protections

Notice Of Privacy Practices

- Purpose is to inform patients about kinds of uses and disclosures of PHI that may occur, their rights with respect to the PHI, and the covered entity's duties under the rule
- Plain language
- Specified elements
- Complaints
- Contact person
- Revisions (going forward only)

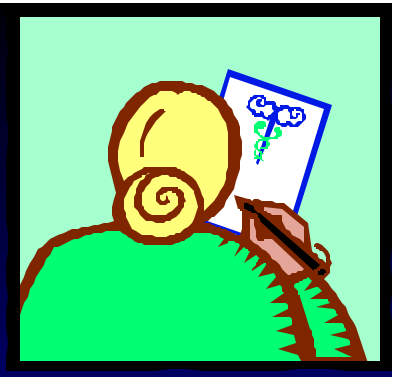
Notice Under the March 2002 Proposal

- Notice is more important under March 2002 changes
  - Good faith effort to obtain individual's written acknowledgement of receipt of Notice
  - Not applicable to indirect treatment providers
  - No standards for how provider obtains the patient's acknowledgement

Access, Inspection, And Copying

- See and make copies of records
- Facility must respond within 30 or 60 days
- Facility may deny requests under limited circumstances
- Psychotherapy notes excluded

Accounting Of Disclosures



- All disclosures of PHI other than for treatment, payment, or health care operations
- Specified elements
- Patient entitled to receive accounting for previous 6 years
- Facility must respond within 60 days
- Patient entitled to one free accounting per year
- Facility must document disclosures, the written accounting given to patients, and the name and title of the person in the facility responsible for handling requests

Request Amendments

- Patients have the right to request amendments
- Under some circumstances, facility may deny patient's request
- Procedures to follow for requesting amendments and responding to requests
- Facility must act on a request within 60 days

Restrict Disclosures

- Patients have the right to request that the facility restrict the use or disclosure of PHI
- Facility may choose not to grant the request
- If the facility agrees, is it bound
- Facility must establish policies and procedures to deal with requests

Request Privacy Protections

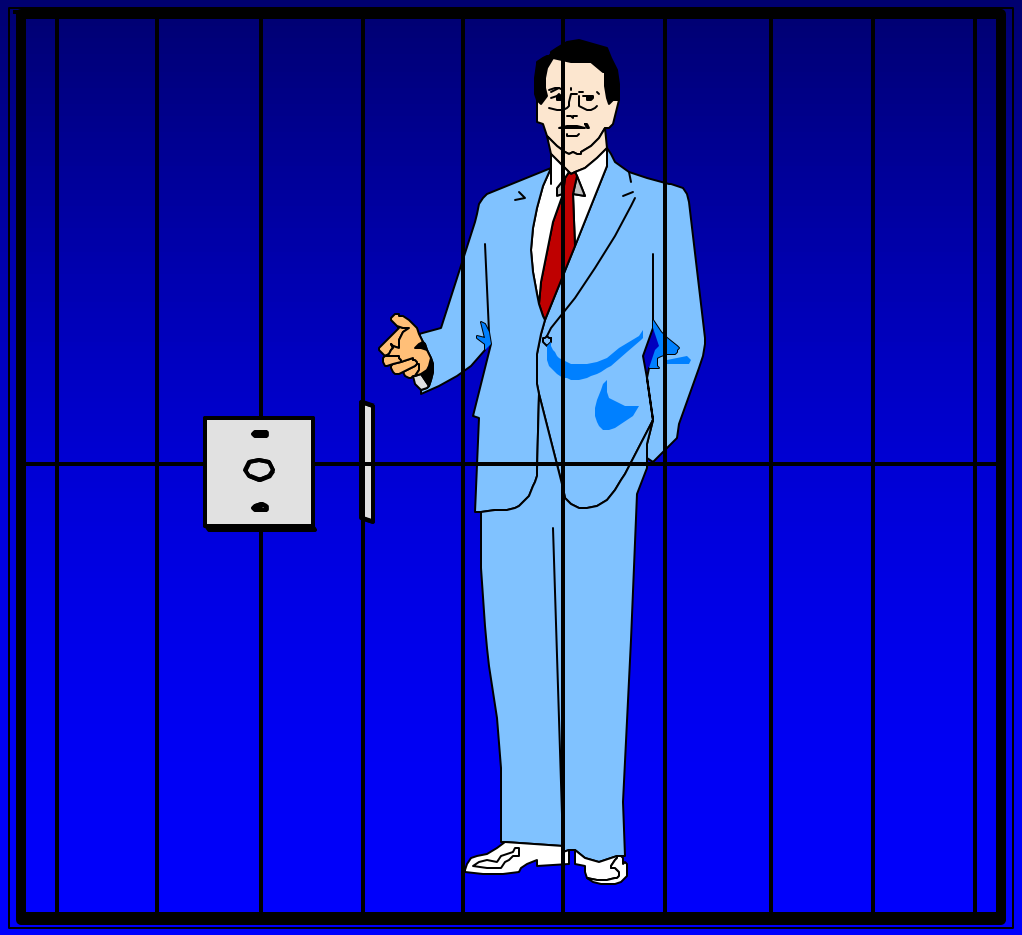
- Patients may request that the provider communicate PHI by alternative means or at alternative locations.
  - Example: if a patient does not want his family to know that he is receiving treatment, he may request that the facility send all communication to his work address.
- Facility must accommodate reasonable requests.

Administrative Requirements

- Designation of a “Privacy Official”
- Policies and Procedures
- Training
- Reporting and complaint processing mechanism
- Sanctions
- Duty to mitigate

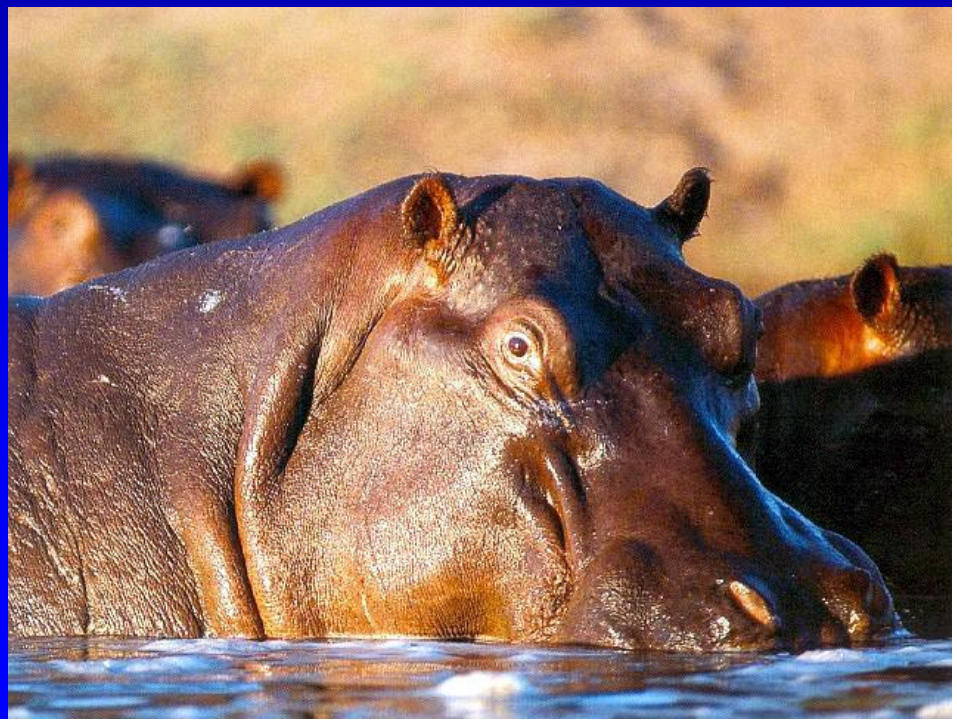
Enforcement Efforts

- Prison and fines
- HHS Office of Civil Rights
- Guidance



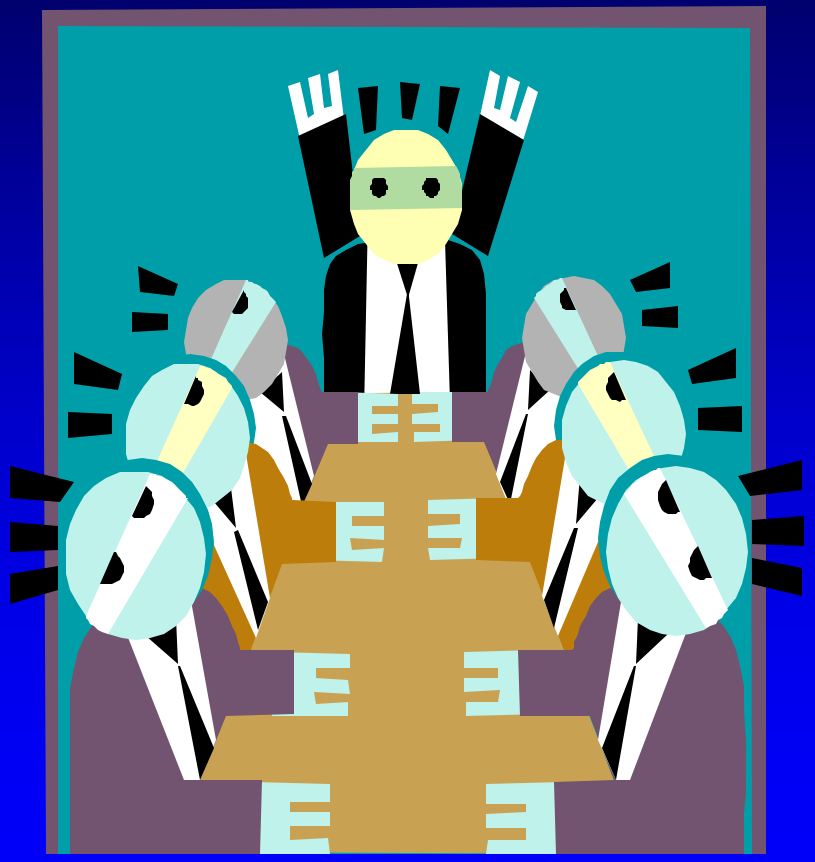
The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)

Implementation



Getting Started

- Identify HIPAA organizational structure(s)
- Create a “Privacy Task Force”
- Determine scope of the project
  - HIPAA
  - state privacy law
  - corporate compliance
- Conduct an assessment and inventory



Compliance Strategy

- Inventory uses of PHI
- Identify covered entities and business associates
- Develop and implement privacy procedures
- Develop and implement privacy procedures with business associates
- Monitor state laws

Thank You!

Michael D. Bell, Esq.
Mintz, Levin, Cohn, Ferris,
Glovsky and Popeo, P.C.
Washington, D.C.
(202) 434-7481
mbell@mintz.com

MINTZ LEVIN
COHN FERRIS
GLOVSKY AND
POPEO PC