

A collection of medical instruments, including a stethoscope, a reflex hammer, and a tongue depressor, arranged on a light-colored surface. The stethoscope is coiled, the reflex hammer is positioned vertically, and the tongue depressor is placed horizontally across the center.

Privacy for Compliance Professionals

Michael D. Bell, Esq.

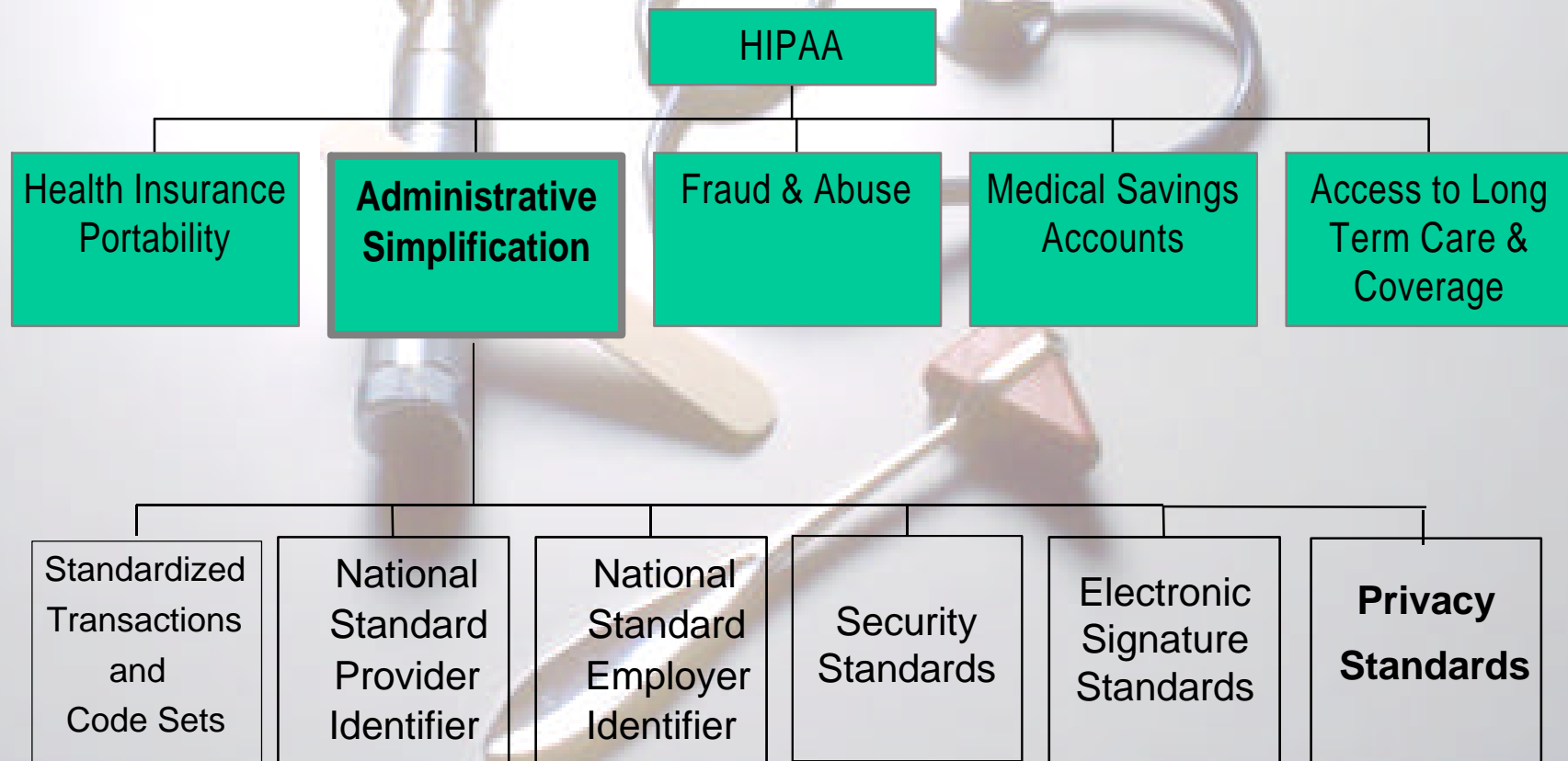
Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.

Washington, DC

202-434-7481

Mbell@mintz.com

The Multiple Components of HIPAA



Recent HIPAA News



- On December 27, 2001, President Bush signed into law the **Administrative Simplification Compliance Act**.
- By October 16, 2002, covered entities, including pharmacies, 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.

A collection of medical instruments, including a stethoscope, a reflex hammer, and a tongue depressor, arranged on a light-colored surface. The stethoscope is at the top, the reflex hammer is at the bottom right, and the tongue depressor is in the middle left.

Proposed Security and Electronic Signature Standards

Overview

Security Standards

A collection of medical instruments including a stethoscope, a reflex hammer, a reflex mallet, and a reflex hammer, arranged in a circular pattern around the text.

4 Components

- Administrative
- Physical
- Technical Services
- Technical Mechanisms

UPDATE

- HHS OCR has reported that the final version of the Security and Electronic Signature Standards have been forwarded to OMB for final review and should be released before the end of the year.



Standards for Privacy of Individually Identifiable Health Information

Overview of the “Privacy Regulations”

A stethoscope, a reflex hammer, and a reflex mallet are arranged on a light-colored surface. The stethoscope is positioned at the top, with its chest piece facing right. The reflex hammer is in the center, with its head pointing towards the bottom left. The reflex mallet is at the bottom, with its head pointing towards the bottom left.

“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.

Covered Entities



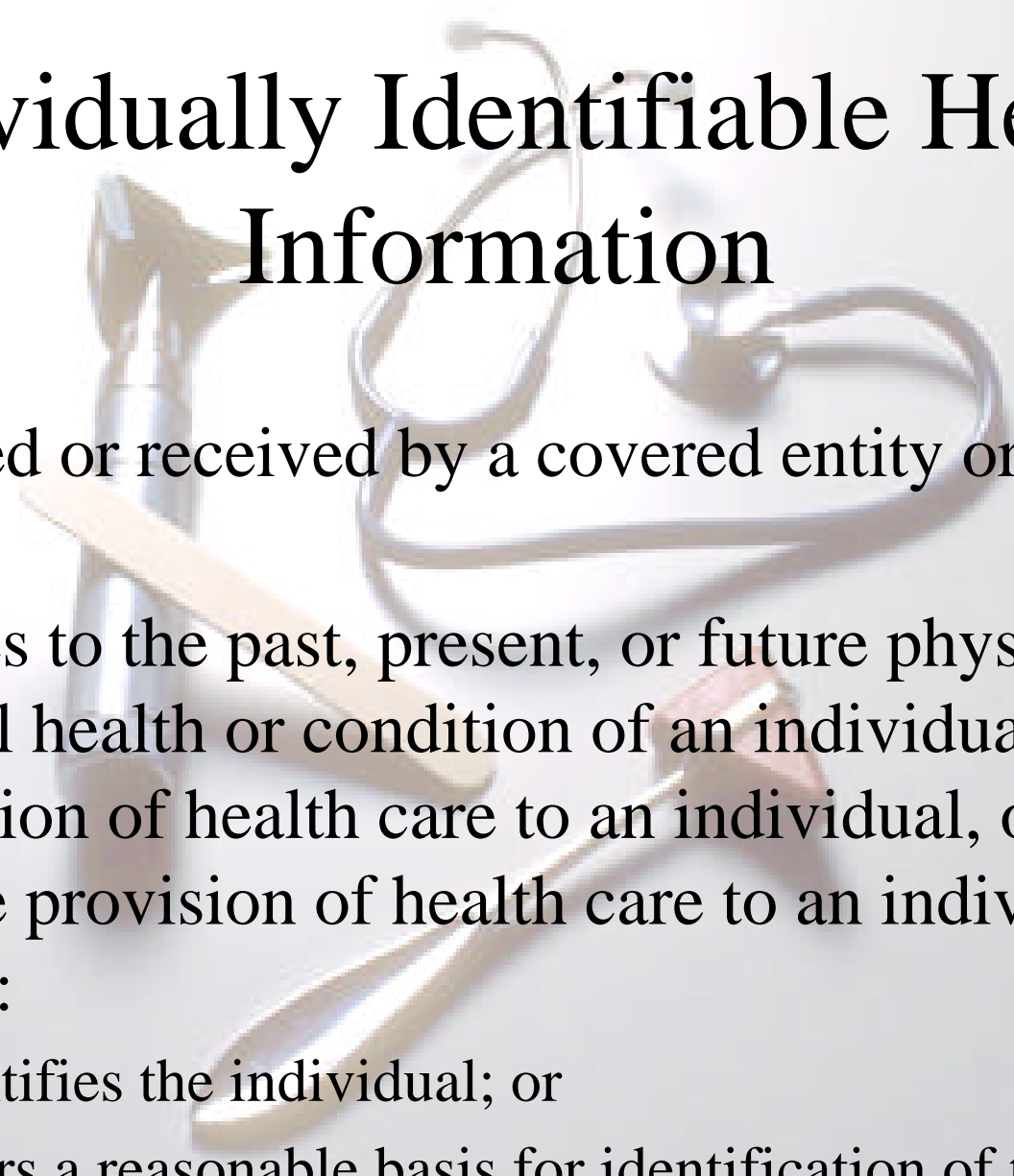
- **Covered entities**
 - health plans;
 - health care clearinghouses; and
 - providers that transmit health information in electronic form in connection with a HIPAA standardized transaction
- Also reaches indirectly the “Business Associates” of the covered entity

Protected Health Information (PHI)

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



Individually Identifiable Health Information

A collection of medical instruments, including a stethoscope, a reflex hammer, and an otoscope, are arranged on a light-colored surface. The stethoscope is coiled, and the reflex hammer and otoscope are positioned diagonally across the frame.

- 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

Uses and Disclosures of PHI

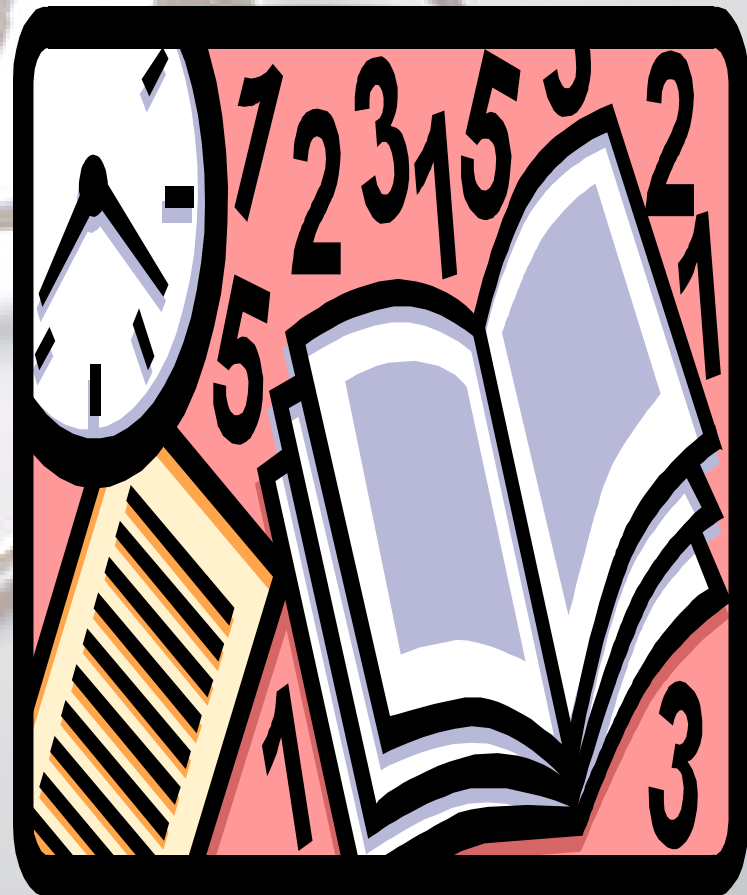
A faint, artistic background image featuring a medical stethoscope and a reflex hammer, suggesting a healthcare setting.

- Four categories of uses and disclosures of PHI
 - **Consent required**—direct treatment providers—treatment, payment, and health care operations
 - **Oral agreement required**—facility directories and disclosures in the presence of personal care givers
 - **No consent, authorization or agreement required**—required by law, for public health activities, etc.
 - **Authorization required**—all other uses and disclosures

General Rules for Uses and Disclosures

Minimum Necessary

Business Associates



Minimum Necessary

- Covered entities must limit the PHI used or disclosed to the minimum necessary to achieve the purpose of the use or disclosure.
 - doesn't apply to disclosures made for treatment or to the individual
- Identify persons or classes of persons who need access to PHI, and the categories of PHI that they need access to, in order to carry out their duties.



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.
- Covered entities are required to execute agreements with each of their business associates to ensure that PHI provided to business associates is protected in the same manner as required of the covered entity.



Patient Rights

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

Administrative Requirements

A collection of medical and administrative tools including a stethoscope, a reflex hammer, a pen, and a wooden tongue depressor, arranged on a light gray background.

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

Getting Started

A collection of medical instruments is arranged on a light-colored surface. A stethoscope with a silver chest piece and black tubing is positioned in the upper right. A reflex hammer with a wooden handle and a metal head is in the lower right. An otoscope with a silver handle and a black ear speculum is in the lower left. The instruments are slightly out of focus, creating a soft, professional background for the text.

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

Compliance Integration

7 Elements of a Corporate Compliance Program

HIPAA Security Requirements

HIPAA Privacy Requirements

Policies and Procedures	Administrative Procedures	Documentation of Policies and Procedures
Assignment of Oversight Responsibilities	Assigned Security & Privacy Responsibility	Designated Privacy Official
Training and Education	Training and Education	Training
Lines of Communication	Report Procedures; Event Reporting	Complaint Processing
Enforcement and Discipline	Sanctions	Sanctions
Auditing and Monitoring	Internal Audit	Accounting for Disclosures
Response and Corrective Action	Response Procedures; Testing & Revision	Duty to Mitigate

Organizational Structures

- A “**hybrid entity**” or “**component entity**” means a single legal entity that is a covered entity and whose “covered functions” are not its primary functions
- **Affiliated 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

A collection of medical instruments, including a stethoscope, a reflex hammer, and a tongue depressor, arranged on a light-colored surface. The stethoscope is positioned at the top, with its tubing and chest piece visible. The reflex hammer is in the center, and the tongue depressor is at the bottom. The background is a soft, out-of-focus light gray.

Privacy Task Force

- Privacy Officer--responsible for the development and implementation of the policies and procedures of the covered entity
- Task force--assists with the development and day-to-day operations of the Privacy Program

Project Scope

A collection of medical instruments is arranged on a light gray surface. A silver stethoscope is positioned in the upper right, with its tubing coiled. A wooden tongue depressor lies horizontally across the middle. A reflex hammer with a wooden handle and a metal head is positioned diagonally in the lower right. A silver pen or marker is visible on the left side, partially obscured by the tongue depressor.

- HIPAA
- State statutes, regulations, and common law
- Other federal privacy laws (e.g., COPPA)
- Corporate Compliance

Privacy Assessment



- Identify
 - the flow of PHI throughout the covered entity
 - data elements within the record
 - the purposes for uses and disclosures
 - whether there is a sale of data
 - the retention period for data
 - the final disposition of the data
 - the instrumentality
- Gather existing policies and procedures
- Identify available infrastructure
- Compare your findings to the requirements set forth in the regulations and state statutory, regulatory and common law

A collection of medical instruments is arranged on a light gray background. A silver stethoscope is coiled in the upper right. A reflex hammer with a silver head and a wooden handle is positioned vertically on the left. A wooden tongue depressor lies horizontally across the center. A reflex hammer with a red handle is partially visible in the lower right.

THANK YOU

Michael D. Bell, Esq.

Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.

202-434-7481

mbell@mintz.com