

Shelby County Government

Overview of HIPAA Revisions

Presented By: Johnson Saulsberry

Improved Privacy and Security Provisions

- Broader HIPAA Scope of Coverage
- Federal Security Breach Notifications Requirement
- Additions & Modifications to certain HIPAA Requirement
- New HHS Inspection & Enforcement Framework
- New tiered penalties for federal & state regulators
- Varying effective dates for different sections

Broader HIPAA Scope of Coverage

- Health Plans
- Health Care Clearinghouse
- Health Care Providers who conduct certain health care transactions electronically
- **Business Associates**
- **Other third parties who are not business associates (under a forthcoming evaluation)**

Broader HIPAA Scope of Coverage

Highlight

Business Associates and other third parties are subject to the same HIPAA administrative, Physical, and technical security controls and penalties as covered entities

Impact/Risk

Contract BAA updates

BA compliance programs

Security Breach Notifications

Breach Definition

An individual's protected health information that has been, or is reasonably believed by the covered entity to have been accessed, used, acquired or disclosed to an unauthorized person, except where an unauthorized to whom such information disclosed would not reasonably have able to retain such information. It includes information in any format – paper, tapes, electronic, etc.

Exceptions:

Unintentional access by employees or individuals acting under authority of covered entity or business associate if information is not used or further disclosed.

Security Breach Notifications for “unsecured” health information

- Covered entities must promptly notify (within 60 days) individuals whose “unsecured” health information may have been disclosed as a result of a security breach

Notification must include:

- date of breach and date of discovery of breach
 - type of protected health information involved
 - steps individuals should take to protect themselves
 - steps the covered entity is taking to mitigate harm and protect against future breaches
- If more than 500 people are affected, the covered entity must notify a prominent media outlet serving the state or jurisdiction and HHS immediately
 - The covered entity must notify the HHS annual for breach less than 500
 - Business Associates must notify Covered Entity including the identity of each individual involved
 - HHS will list breaches involving more than 500 on its website
 - Similar requirement for Personal Health Records (PHR) vendors, with reporting to the Federal Trade Commission (FTC)

Does not Apply

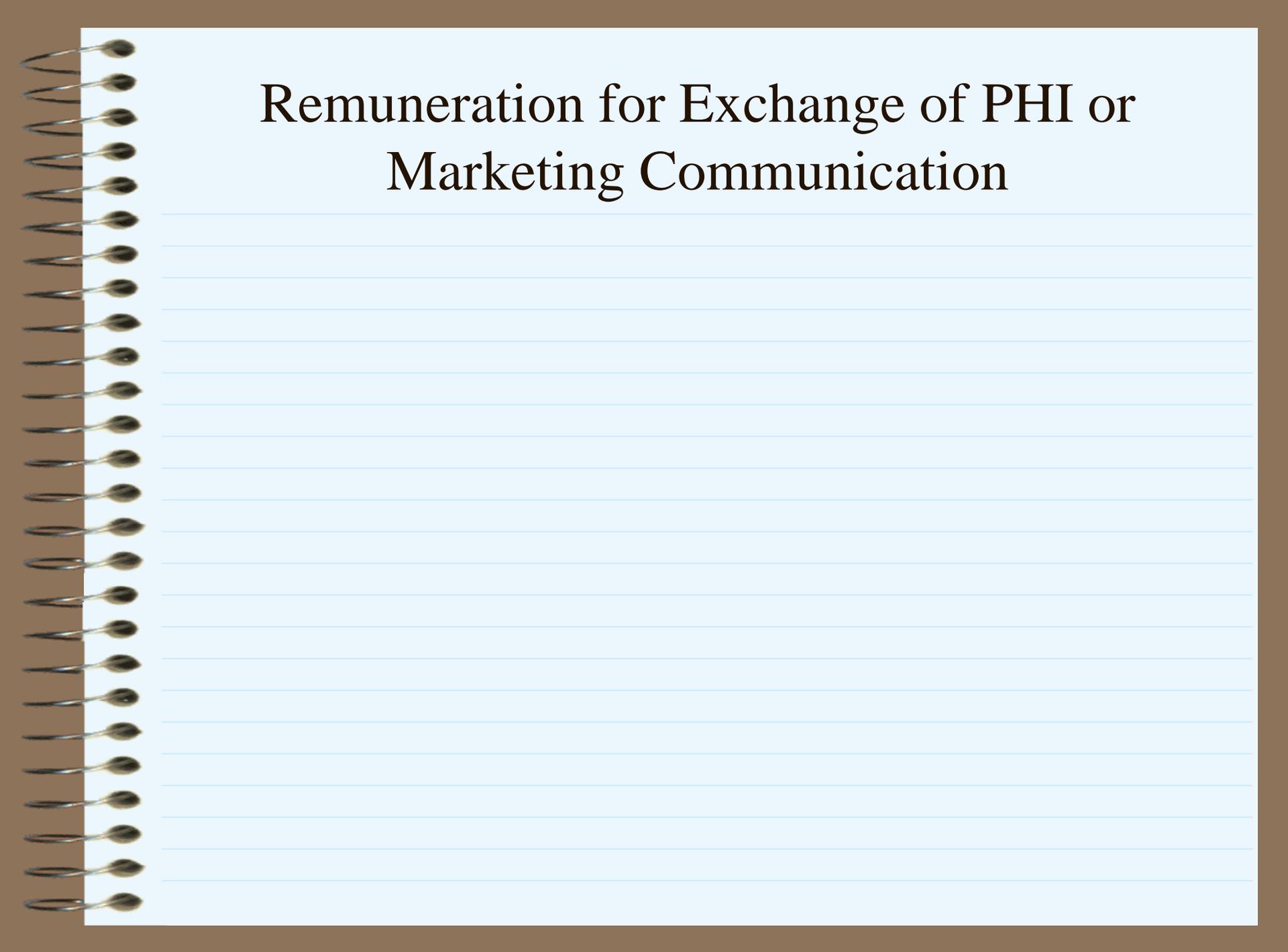
- Standards for Encryption & Disposal of PHI

Additions & Modifications to certain HIPAA Requirement

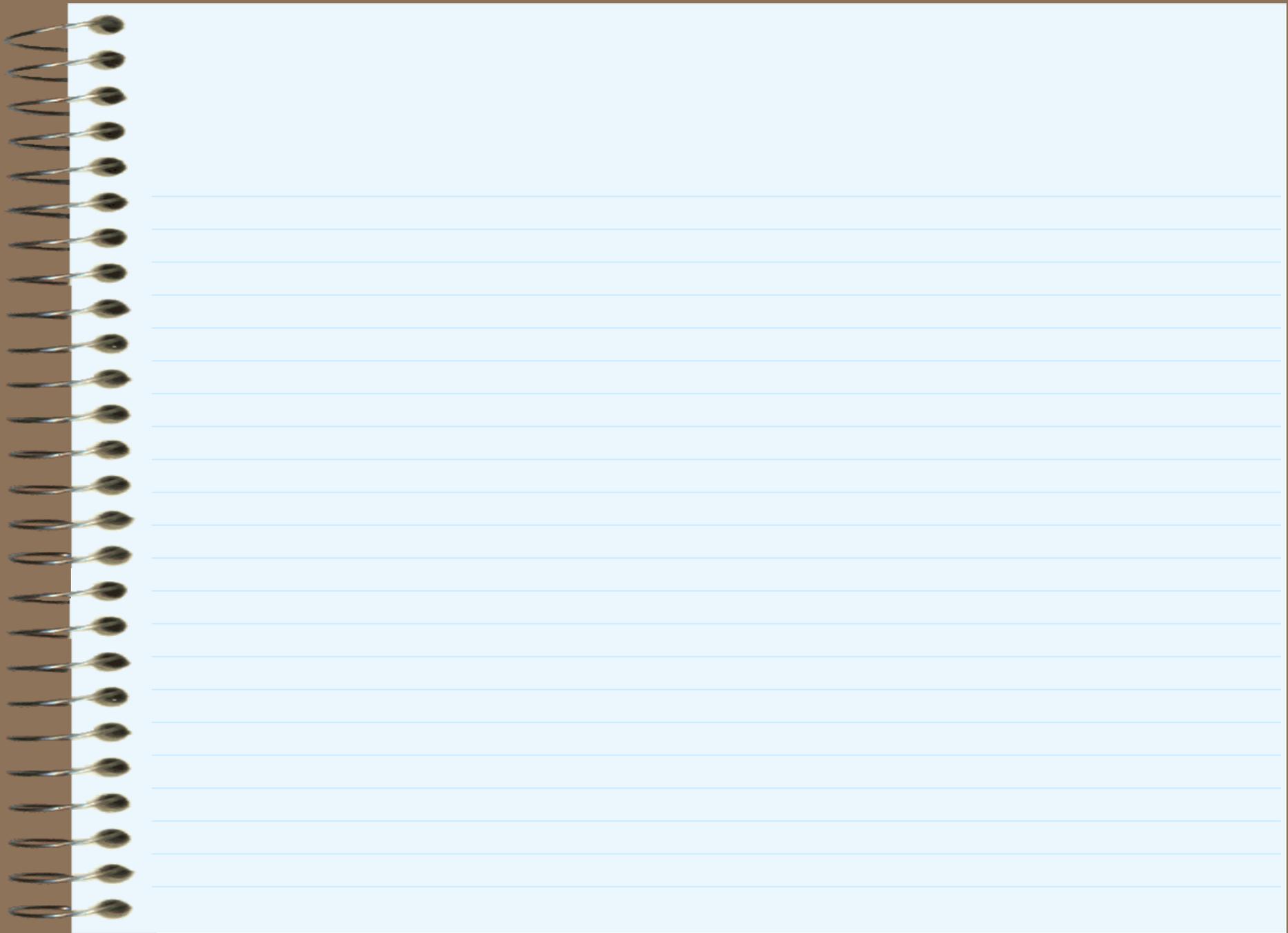
- Disclosure Log – now includes treatment, payment and healthcare operations
- Patient access rights – electronic records, 3 years for accounting
- Patient access rights to information from Business Associates
- Minimum Necessary – applies to treatment disclosures
- Additional restriction on use of PHI without a valid authorization

Accounting for Disclosures

- Covered entities that maintains electronic health records must include routine disclosures for treatment, payment or health care operations (TPO) in its accounting list.
- The TPO accounting would be limited to 3 years (accounting or other disclosures would remain 6 years, as under the current rule).

A graphic of a spiral-bound notebook with a brown cover and a white page. The page is ruled with light blue horizontal lines. The spiral binding is on the left side. The title is centered at the top of the page.

Remuneration for Exchange of PHI or Marketing Communication

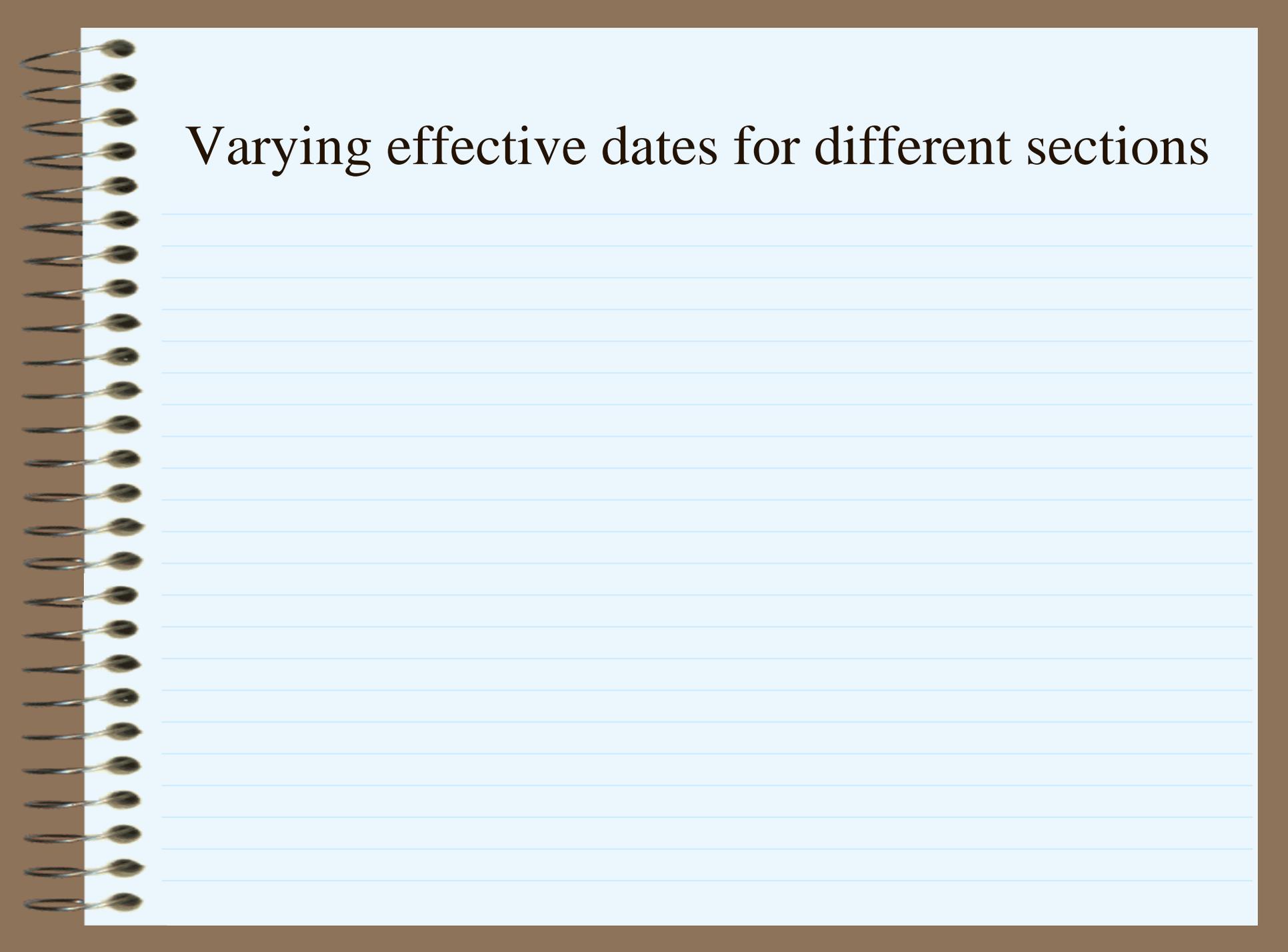


New HHS Inspection & Enforcement Framework

- HHS required to conduct inspections of covered entities
- Inspections of business associates
- Publication of inspections, general findings
- Publication of security breaches of HHS website

New tiered penalties for federal & state regulators

- State General can bring actions for violations
- Individual right to a percentage to the government fine

A spiral-bound notebook with a brown cover and a white page. The page has light blue horizontal ruling. The spiral binding is on the left side.

Varying effective dates for different sections

Recommended Approach to Compliance

- Conduct Security Assessment
- Develop a Security breach notification process
- Review, Revise and Re-executed Business Agreements
- Develop policies & procedure (including Notice of Privacy Practices to accommodate revisions
- Train employees regarding revisions
- Auditing/compliance monitoring

If We Don't Comply



ENFORCEMENT



CIVIL PENALTIES

THE OFFICE OF CIVIL RIGHTS (OCR)

Per Calendar Year

No Knowledge - \$100 - \$25,000
Reasonable Cause - \$1000 - \$100,000
Willful Neglect - \$10,000 - \$50,000
Maximum penalty - \$50,000
Cap - \$1.5 million for identical requirement

CRIMINAL PENALTIES

THE DEPARTMENT OF JUSTICE

Penalties up to \$250,000
Prison time up to 10 years

**OPPORTUNITY
FOR
QUESTIONS**

