HIPAA Administrative Simplification Enforcement Rule

Highlights of the Final Rule

Presentation to NCVHS

April 4, 2006

Carol C. Conrad, J.D.

Office of General Counsel

Department of Health & Human Services

Enforcement Rule Vital Statistics

- Proposed rule published April 18, 2005 at 70 FR 20224.
  - Comment period closed on June 17, 2005.
  - 49 public comments, mainly from health care entities and industry groups.
- Final Enforcement Rule was published February 16, 2006 at 71 FR 8390. It was effective on March 16, 2006.
- The final rule –
  - Replaces prior rules at 45 C.F.R. Part 160, Subpart C (complaint and investigation procedures) and Subpart E (interim final procedural rules).
  - Adds a new Subpart D (imposition of civil money penalty).

To Whom Does The Enforcement Rule Apply?

- Entities covered by the HIPAA rules – a.k.a., "covered entities."
- HIPAA rules: Privacy Rule, Security Rule, Transactions Rule, identifier rules (the NPI and EIN Rules to date, the NPlanID Rule to come). The comment period on the proposed Claims Attachment Rule closed on January 23.
- Covered entities are mainly health plans, health care clearinghouses, and health care providers who conduct certain transactions electronically.

What Does The Enforcement Rule Do?

- It establishes the **procedural rules** for –
  - The investigation and informal resolution of compliance issues.
  - The imposition of a civil money penalty (CMP), when a compliance issue is not resolved informally.
- It establishes the **substantive rules** for determining violations and CMPs.
- The procedural rules are in Subparts C, part of Subpart D, and Subpart E of 45 C.F.R. Part 160; the substantive rules are generally in Subpart D.

Procedural Rules: Overview

- The Enforcement Rule provides a uniform enforcement approach for all HIPAA rules.
- The Enforcement Rule adapts the CMP rules of HHS's Office of the Inspector General as the procedural framework for the Enforcement Rule.
- The Enforcement Rule establishes a two-stage enforcement process –
  - An informal stage, where compliance is investigated and the case may be resolved informally.
  - A formal stage, which occurs when a compliance dispute is not resolved informally. This stage usually consists of a formal administrative hearing and an appellate process, leading either to imposition of a CMP or a formal finding that the proposed CMP may not be imposed.

Procedural Rules – Investigation And Compliance (Subpart C)

- The final rule revises Subpart C to apply the compliance and enforcement procedures of the Privacy Rule to all of the HIPAA rules.
- Subpart C describes the procedures for investigations and the informal resolution of compliance issues. An informal resolution may be reached by demonstrated compliance or a corrective action plan or other agreement.
- Prior to concluding that an informal resolution cannot be reached, HHS will give the covered entity a chance to demonstrate mitigating factors or affirmative defenses that would bar a CMP.

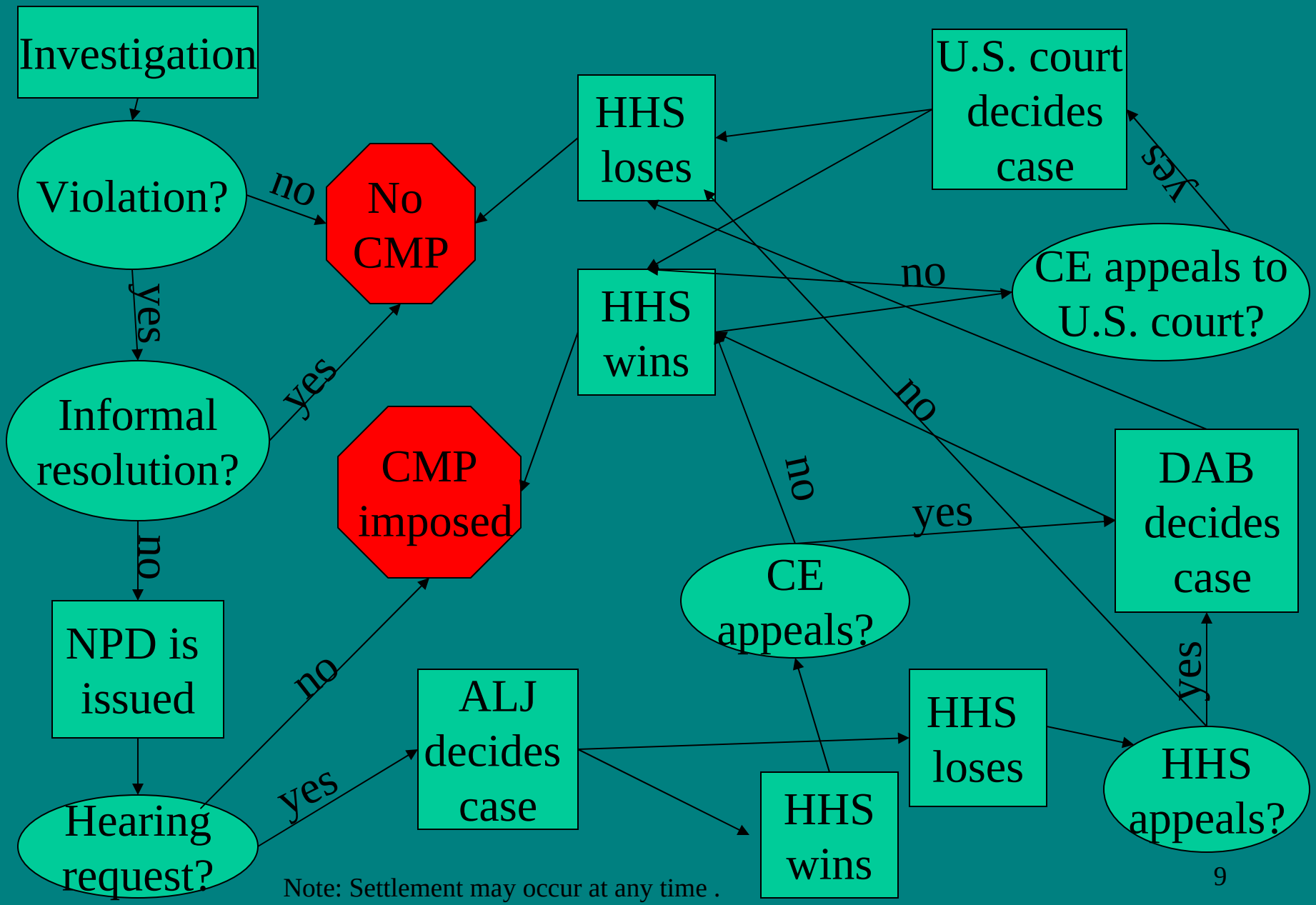
Procedural Rules – Imposing A CMP (Subpart D)

- If a violation is found and not resolved informally, OCR or CMS will issue a "Notice of Proposed Determination" (NPD) stating the violation(s) found, the CMP proposed, and the facts and law justifying the proposed CMP.
- The covered entity may challenge the proposed CMP, by requesting a hearing.
  - If the covered entity requests a hearing, a formal administrative hearing process before an administrative law judge (ALJ) ensues.
  - If the covered entity does not request a hearing, the proposed CMP becomes final and subject to collection.

Procedural Rules – Hearing Process (Subpart E)

- If a covered entity wishes to challenge a proposed CMP, it must request a hearing.
- An ALJ will hear the agency's and the covered entity's arguments and evidence, and decide the case.
- The hearing process resembles a judicial trial, but is less complex.
- Either party may appeal the ALJ's decision to a panel of the Departmental Appeals Board (DAB).
- The DAB's decision becomes the Secretary's decision; only the covered entity may appeal it to federal court.

HIPAA Enforcement Process Overview



Note: Settlement may occur at any time .

Substantive Rules – Overview

- The Enforcement Rule establishes the substantive rules for determining the liability of a covered entity for a CMP and the amount of a CMP.
- The substantive rules interpret the CMP part of the HIPAA statute and answer several questions:
  - On what basis will HHS impose a CMP?
  - What is a violation?
  - When is a covered entity liable for acts by others?
  - How is the amount of a CMP determined?
  - What affirmative defenses may a covered entity raise to bar imposition of a CMP?
- These rules are mostly in Subpart D; however, the definition of “violation” is in Subpart C.

General Rule

- HHS will impose a CMP if it determines that the covered entity has violated an administrative simplification provision, unless an affirmative defense applies.
- Imposition of a CMP is not always required when a violation has occurred. For example, a CMP is not required when –
  - The case is informally resolved.
  - An affirmative defense applies.

What Is A Violation?

- A “violation” is a failure to comply with an administrative simplification provision.
- An “administrative simplification provision” is a requirement or prohibition of HIPAA or a HIPAA rule.
  - An administrative simplification provision may, but need not, be part of a standard or implementation specification.
  - A standard or implementation specification may contain more than one administrative simplification provision.
- In most cases, the particular violation will be a failure to comply with one of the other HIPAA rules (e.g., the Privacy Rule) rather than the Enforcement Rule itself.

Vicarious Liability Of A Covered Entity For A Violation

- By statute, a covered entity is liable for the acts of its agents within the scope of the agency. This principle applies to –
  - Workforce members, to the extent they are agents and act within the scope of their agency.
  - Business associate agents acting within the scope of their agency, unless the covered entity is in compliance with the business associate provisions of the Privacy or Security Rule, as applicable, with respect to the business associate agent.
- Agency issues will be determined by the federal common law of agency.

Calculating A CMP

- General rules for calculating CMPs:
  - The amount of the penalty is calculated in accordance with §§ 160.406 (determining the number of violations), 160.408 (amount of penalty for the violation based on aggravating and mitigating factors), and 160.412 (waiver).
  - The maximum amount per violation and for identical violations in a calendar year may not exceed the statutory caps: $100/violation and $25,000/identical violations in a calendar year.
- The regulation prescribes general principles, not a rigid formula, for calculating a CMP.

Counting Violations

- Identical violations are counted "based on the nature of the covered entity's obligation to act or not act under the provision that is violated …".
  - This may require considering the number of persons affected, applicable time limits, particular contract provisions, etc.
  - Continuing violations are to be counted in days.
- One act may violate both a specific and a general provision of a HIPAA rule. This would be counted as one, rather than two, violations.

Aggravating And Mitigating Factors

- By statute, HHS must consider aggravating and mitigating factors in determining the amount of a CMP. The particular factors that HHS may consider are set out in Subpart D.
- The regulatory factors are –
  - General, e.g., "the degree of culpability of the covered entity" or "such other matters as justice may require."
  - Not designated as aggravating or mitigating. They will have to be interpreted and applied as appropriate to the circumstances.
- These factors will be used to justify the penalty amount/violation, which may not exceed $100.

Affirmative Defenses

- Three statutory limitations on imposition of a CMP:
  - The act is a criminal offense under HIPAA;
  - The covered entity lacked knowledge of the violation; or
  - The violation was due to reasonable cause and not willful neglect and is timely corrected.
- These limitations are treated as affirmative defenses, meaning that if they are shown to exist, HHS may not impose a CMP, even though the violation occurred.
- As affirmative defenses, the covered entity has the burden of proving them.

Other Provisions Of Interest

- If a CMP is imposed, HHS will inform various state and other agencies and organizations and the public of the CMP.
- Covered entities are prohibited from taking retaliatory acts or intimidating persons who cooperate or participate in the enforcement process. Such acts constitute a violation and are a basis for a CMP.
- There are provisions for protecting protected health information obtained in an investigation or used in the course of the hearing process.