How to Effectively Respond to an OCR HIPAA Privacy Complaint Investigation

Mark Rogers

The Rogers Law Firm

HIPAA Privacy Enforcement

- Civil and Criminal Penalties for violation of the HIPAA Privacy Rule
    - Civil Penalties = Office for Civil Rights (OCR)
        - Violation of the HIPAA Privacy Standards
    - Criminal Penalties = Department of Justice
        - "Knowingly": (1) uses or causes to be used a unique health identifier;
          (2) obtains individually identifiable health information relating to an individual; or
          (3) discloses individually identifiable health information to another person.

HIPAA Privacy Enforcement

- Secretary of HHS delegates the following duties to the Office for Civil Rights (OCR):
  - Administer the HIPAA Privacy Standards;
  - Authority to impose Civil Monetary Penalties for failure to comply with HIPAA Privacy Standards;
  - Authority to make state law preemption determinations; and
  - Authority to make decisions regarding the interpretation, implementation and enforcement of the Privacy Standards.
    - » 65 Fed. Reg. 82,381 (Dec. 28, 2000)

HIPAA Privacy Enforcement

- Civil Penalties
  - $100 penalty for each violation of the Privacy Standards
  - $25,000 annual cap on civil monetary penalties per type of violation
    - » 42 U.S.C. § 1320d-5

HIPAA Privacy Enforcement

- Final HIPAA Enforcement Rule
  - » 71 Fed. Reg. 8390 (February 16, 2006)

  - – Sets forth the bases and procedures for imposing civil monetary penalties on covered entities that violate any of the administrative simplification provisions of HIPAA

  - – "If a finding of violation is made, a civil monetary penalty will be sought for a violation…"

  - – Effective: March 16, 2006

HIPAA Privacy Enforcement

- Final HIPAA Enforcement Rule (cont.)
  - Factors which *may* be considered in determining amount of CMP:
    - (a) nature of the violation;
    - (b) circumstances, including the consequences of the violation;
    - (c) degree of culpability of a covered entity;

HIPAA Privacy Enforcement

- Final HIPAA Enforcement Rule (cont.)
  - (d) history of prior compliance with the administrative simplification provisions;
  - (e) financial condition of the covered entity; and
  - (f) such other matters as justice may require.

HIPAA Privacy Enforcement

- Final HIPAA Enforcement Rule (cont.)
    - Potential of multiple CMPs for a single violation
    - For a violation which implicates multiple administrative simplification provisions… “we see no reason why they should not be considered as separate violations, since covered entities must comply with all applicable requirements and prohibitions of the HIPAA provisions and rules.”

HIPAA Privacy Enforcement

- Final HIPAA Enforcement Rule (cont.)
    - Covered entities are liable for HIPAA violations by workforce members, including employees and independent contractors
    - Business Associates?

HIPAA Privacy Enforcement

- Statistics
  - July 2003 through October 31, 2006:
    - 23,268 complaints received by OCR
    - 76% were “resolved”
    - No fines imposed
    - OCR referred 346 complaints to DOJ
    - Top targets: private healthcare practices, hospitals, outpatient facilities, group health plans, and health insurers
      - » Melamedia’s *Health Information Privacy/Security Alert*

HIPAA Privacy Enforcement

- Statistics (cont).
  - Top five complaints received by OCR:
    - Impermissible use or disclosure of an individual’s identifiable health information;
    - Lack of adequate safeguards to protect identifiable health information;
    - Refusal or failure to provide the individual with access to or a copy of his or her records;
    - Disclosure of more data than is minimally necessary to satisfy a request for information; and
    - Failure to have the individual’s valid authorization for a disclosure that requires one.
      - » Melamedia’s *Health Information Privacy/Security Alert*

Responding to the OCR Letter

- “Dear Privacy Officer…”
  - – Very non-specific letter in terms of allegations:
    - – (e.g. “The complaint alleges your entity has not provided a complete copy of the complainant’s medical records nor responded to his complaint regarding the matter. The allegation could reflect violations of 45 C.F.R. §§ 164.524 and 164.530(d) respectively.”)

Responding to the OCR Letter

- OCR authority to collect information and ascertain a covered entity’s compliance is found at 45 C.F.R. §§ 160.300-160.312.

- Covered entities must cooperate with OCR during a complaint investigation (45 C.F.R. § 160.310 (b)) and permit OCR access to its facilities, records and other information during normal business hours at any time, without notice, if exigent circumstances exist (45 C.F.R. § 160.312 (c)).

Responding to the OCR Letter

- “We will contact you within the next two weeks to discuss whether this matter may be resolved without the need for a formal investigation.”

- **Step One**: Do Not Wait! Contact the assigned OCR Investigator. Ascertain the specifics of the allegations set forth in the Complaint.

Responding to the OCR Letter

- **<u>Step Two</u>**: Privacy Officer should notify appropriate individuals:
  - Provider(s) involved
  - President’s Office
  - General Counsel
  - Risk Management Office
  - Insurer (depending upon the circumstances)

Responding to the OCR Letter

- **<u>Step Three</u>:** Conduct an investigation.
  - Who conducts the investigation?
  - How extensive should the investigation be?
  - Gather the appropriate documents (assume OCR has nothing)
  - Document the investigation

Responding to the OCR Letter

- **Step Four**: Draft the formal response
  - Cooperate to the fullest extent possible
  - Give OCR the “full-story”
  - Attach applicable policies and documents to the formal response

Responding to the OCR Letter

- **<u>Step Four (cont.)</u>**:
  - Take a position
  - If fault lies with the covered entity, set forth the proposed remedial measures to be instituted (e.g. policy changes; amendments to forms; following-up with the Complainant)

Responding to the OCR Letter

- **<u>Step Four (cont.)</u>**:
  - Affirm the covered entity’s willingness to fully cooperate with OCR
  - Provide a contact person to OCR (i.e. Privacy Officer and potentially General Counsel’s Office)

Responding to the OCR Letter

- **<u>Step Five</u>**: File the Response
  - – Circulate a draft of the response letter within the institution
  - – File the letter with OCR

OCR Response

- May come in the form of a telephone call to the Privacy Officer or General Counsel seeking further information

- Hopefully, OCR resolves the matter through a formal written response to the covered entity and the complainant

Additional Things to Think About…

- Self-Disclosure?

- Document, Document, Document!!!

- Do not keep others in the dark about remedial measures

- If fault lies with the Covered Entity- make sure it does not happen again

Questions?