Responding to a HIPAA Investigation—What to do When OCR Comes Knocking?

Marc D. Goldstone, Esq.
Hoagland, Longo, Moran, Dunst & Doukas, LLP
40 Paterson Street
P.O. Box 480
New Brunswick, NJ 08903
732-545-4717
732-545-4579 (fax)
MGOLDSTONE@HOAGLANDLONGO.COM
First Step

Don’t Panic!!!!

Really. Prosecutors “home in” on people who “look guilty” (ever watch NYPD Blue?)
Next Step

Call:

- Your Attorneys
- Your Executive Management
- Your Privacy Officer
- Your Security Officer
- Your Compliance Officer
- Your Health Information Management Department/Custodian of Records
On April 17, 2003, the first “Interim” Enforcement Regulations were published (Per DHHS, intended to be the “first installment of a rule” called the “Enforcement Rule.” 68 FR 18895), to be effective 5/19/03.

DHHS intends to REVISE the interim rule by 9/16/04 (corrected from initially published expiration date of 9/16/03; 68 FR 22453).

There are no HIPAA HIPPOs (Health Information Protection Police Officers) YET!
How Will OCR Enforce HIPAA?

1. **A “Kinder and Gentler” OCR?** “To the extent practical, OCR will seek the cooperation of covered entities in obtaining compliance with the Privacy Rule and may provide technical assistance to help covered entities voluntarily comply”--“enforcement activities will focus on obtaining voluntary compliance through technical assistance. 68 FR 18897

2. **The Government is Here to Help:** “OCR will seek to resolve matters by informal means before issuing findings of non-compliance” Id.
OCR Enforcement-Con’t

3. **Does Anyone Like a Rat?** “The process will be *complaint-driven* and consist of progressive steps that will provide opportunities to demonstrate compliance or submit a corrective action plan. 68 FR 18897
If OCR Knocks At Your Door

- Cooperate (but cautiously!) Ask for the official identification of the investigators (NOT business cards); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. TIP-if they can’t produce acceptable I.D., call your attorney immediately and defer the provision of any PHI-but BE SURE before you do.

- Ask for the name and telephone number of their supervisors (if their demeanor permits)

- Be sure to determine if there are any law enforcement personnel present (i.e, FBI, US Attorney investigators, State Prosecutor investigators, etc.)

- Permit the investigators to have access to PHI.
What To Do While They’re At Your Office

- Ask for copies of any search warrants and/or entry and inspection orders
- Ask for copies of any complaints
- Ask for a list of patients they are interested in
- Ask for a list of documents/items seized
- Do NOT expect that they will give you any of the above, except for the search warrant and a list of items seized (if any).
Anything Else To Do?

- Don’t leave them alone, if possible (assign an employee to “assist” each investigator)
- Don’t be TOO solicitous
  - Don’t offer food (“WCD” rule)
  - Don’t get “chatty”; anything you say REALLY CAN be used against you!
- Keep your employees away from the central office
- Notify the Association (if you feel comfortable, to obtain their help and also to help “spread the word”)

Responding to an Investigation (c) 2003 Marc D. Goldstone, Esq.
Will You Have Advance Notice?

- Maybe-Maybe not.

  - Remember-Anyone may file a complaint with OCR; the complainant need not notify the CE.
  - Complaints must be filed within 180 days of when complainant knew or should have known of the violation.
    - Beware that DHHS can extend this time period for "good cause shown".
  - The Secretary "will generally" give notice before requesting access to books and records (65 Fed. Reg. 82602, 12/28/00), but is NOT REQUIRED to do so.
What Will They Do?

- If OCR determines that a CE has committed a HIPAA violation, they will:
  - Inform the Covered Entity (in writing)
  - Inform the complainant (if any, in writing)
  - Per the enforcement rule, OCR SHOULD attempt to resolve the matter by informal means "whenever possible"
  - If the issue cannot be informally resolved, DHHS has the authority to issue a written noncompliance finding.

- If no violation is found:
  - Inform the Covered Entity and the complainant, if any (nothing says this notification must be in writing)
Crimes Against HIPAA?

- What if the violation is egregious enough to constitute a crime?
  - “Secretary shall impose”
    - Criminal Fine: up to $50,000 and/or 1 year in jail
    - Obtain, Use and/or Disclose PHI under false pretenses: up to $100,000 and/or 5 years in jail
    - Intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm:
      - up to $250,000 and/or 10 years in jail

- OCR: Enforces Privacy Rule; criminal issues referred to OIG
Is a HIPAA violation also a violation of the Medicare Conditions of Participation?

- "We have not yet addressed" it; however, "we note that Medicare conditions of participation require participating providers to have procedures for ensuring the confidentiality of patient records".

65 Fed Reg. 82605, 12/28/00
Limits on DHHS CMP Authority

1. CMPs cannot be imposed in respect of acts that constitute a “HIPAA Crime.” 42 USC 1320d-5(b)(1)

2. A CMP may not be imposed if “it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision.” 42 USC 1320d-5(b)(2)
Limits on DHHS CMP Auth.-Con’t

3. A CMP may not be imposed if the failure to comply was due to “reasonable cause and not to willful neglect.” 42 USC 1320d- 5(b)(3)

4. A CMP may be reduced or waived “to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.” 42 USC 1320d- 5(b)(4)
Limits on DHHS CMP Auth.-Con’t

5. Secretary may NOT initiate a CMP action “later than six years after the date” of the occurrence that forms the basis for the CMP. 68 FR 18896.

6. CMP actions are NOT summary; the person upon whom DHHS seeks to impose CMPs MUST be given the written notice and an opportunity for a hearing on the record, where the person may be represented by counsel, may present witnesses, and may cross-examine witnesses. 42 U.S.C. 1320a-7a(c)(2).
Limits on DHHS CMP Auth.-Con’t

7. DHHS CANNOT impose a HIPAA CMP on any person that is NOT a CE! 68 FR 18898 (Are your BAs required to indemnify you for liability imposed on you as a result of their acts/omissions?)
Can You Settle A Case?

- Yes-DHHS can “settle any case or ... compromise any penalty during the process” 68 FR 18898, referencing 45 CFR Part 160.510

- Factors to be taken into account by OCR when making a settlement determination will be “addressed in the notice-and-comment rulemaking” planned for the remainder of the Enforcement Rule. 68 CFR 18899
HIPAA Hearings

- **Timely Requests:** If DHHS notifies a CE of a proposed penalty, the respondent MUST timely request a hearing IN WRITING or the penalty becomes final, and the respondent has “no right to appeal.” 68 FR 18899 referencing 45 CFR Part 160.516.

- **Time Period:** Sixty (60) days after notice of the proposed penalty determination is received by the respondent. 45 CFR Part 160.516 (b)
  - Receipt date is “presumed” to be 5 days after the date of the notice. This is a rebuttable presumption. Id.
HIPAA Hearings-Con’t

- Hearing is on the record 45 CFR Part 160.530(a); 560.
- HHS party will be “OCR and/or CMS” 68 FR 18899
- Discovery is “limited” 45 CFR Part 160.538 (Document production, essentially) Depositions/Interrogatories are specifically prohibited 45 CFR Part 160.538(c)
- Decision of the ALJ is the decision of DHHS 45 CFR Part 160.564 (d) (contrary to many state systems, where an ALJ’s decision can be adopted, modified or rejected by the head of the administrative agency)
- Judicial Review of final penalty decisions is authorized 42 U.S.C. 1320a-7a(e); 45 CFR Part 160.568
- Respondent may request a stay pending judicial review 160.570(a) (file federal appeal papers with ALJ; stay automatically granted until ALJ rules on request)
Penalty Collection

- Penalties are recoverable:
  - in a civil action in U.S.D.C. 45 CFR 160.518(b) (all collateral issues are estopped if they could have been raised by respondent below) 45 CFR 160.518(d)
  - By Offset from “any sum owed … by the United States or a State agency.” 45 CFR 160.518(c).
What to do BEFORE the Investigation?

Be Prepared!

- Implement your HIPAA Compliance Plan to the greatest extent possible (gain HPBs [HIPAA Brownie Points]; make all of your “incidental disclosures” permissible pursuant to the Final Privacy Rule).
- Document the steps that you took to implement your plan; HIPAA committee minutes should be in writing.
- Document the monies you spent in implementing the plan; save budgets and receipts.
- If you made any cost/benefit “reasonableness” determinations regarding specific plan elements, document them and have that documentation available for inspection.
What to do BEFORE the Investigation - Continued

- Periodically examine reports to your Privacy Office/HIPAA Hotline (suggest semi-annually or more)
  - Investigate ALL reports and conclude ALL investigations with WRITTEN documentation (sample form attached)
  - Trend all your reports; if there are discernible trends, conclude them with written documentation.
    - Revisit the trends over time to see if your solution is effective; if not, revise the solution and try again!
- Keep your disclosure logs in good order (especially with respect to inappropriate disclosures-this is where complaints are VERY LIKELY to originate; you don’t want it to appear that you “covered-up” anything!)
What to do BEFORE the Investigation-Continued

- Train, educate, explain, and then train some more
- Maintain employee training time records and training materials used
- Create a “Culture of Privacy” (which probably already exists at most healthcare facilities)
- Watch the online enforcement video from OCR, at http://www.ehcca.com/streaming/index.html

Great guidance from Robinsue Froboese, J.D., Ph.D. Deputy Director, Office of Civil Rights

- Include HIPAA in your policy for responding to official investigations (Don’t have a policy for responding to investigations? Now’s the time to get one!).
What to do BEFORE the Investigation-Continued

- DON’T include the OCR address in your NPP (you don’t have to; you just have to tell patients how to get it. If they have to contact you to get it, then you may have the opportunity to resolve the complaint; at the very least, you’ll be on notice of a potential complaint!)

- GET AND RELY ON THE WRITTEN ADVICE OF COUNSEL/QUALIFIED CONSULTANTS! (at best, they’ll be right; at worst, you can be indemnified by their professional liability policies!) Due diligence is important in developing an effective HIPAA compliance plan.
Thanks!

Thanks for your kind attention!!!!!!!!!!!!!!!!!!!!!!!