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

How Does a HIPAA Complaint Occur?

Does Anyone Like a Rat?

"The process will be ***complaint-driven"*** 68 FR 18897

Can You Do Anything to Mitigate the Damage?

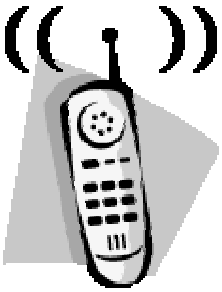
- Don't give up hope! OCR says that the enforcement process will "consist of progressive steps that will provide opportunities to demonstrate compliance or submit a corrective action plan." 68 FR 18897

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

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")

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”.
  - DHHS "will generally" give notice before requesting access to books and records, but is NOT REQUIRED to do so.

What’s the Worst They Can Do?

- If the violation is egregious enough to constitute a “HIPAA Crime”, the “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 IIHI 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. If OIG shows up with a privacy or security complaint, call your lawyers right away!

Even Worse?

- Is a HIPAA violation also a violation of the Medicare Conditions of Participation?
  - The Government states that “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".

What if They Try To Fine You (CMP)?

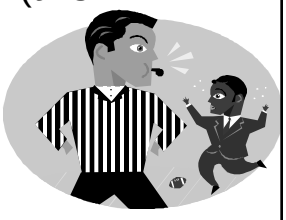
- There ARE defenses to Civil Monetary Penalty (CMP) enforcement, and you should know what they are. The Government has NO CMP authority in these cases:
  - “HIPAA Crime” (2 edged sword)
  - “No Fault” (Didn’t know and could not have known it was a violation)
  - “Reasonable cause and not to willful neglect
  - Penalty “reduced or waived” if excessive in relation to nature of violation
  - Statute of Limitations (6 Years)
  - If You Ask For A Hearing (during the pendency of the proceeding)

Defenses to Fines-Con't

- DHHS CANNOT impose a HIPAA CMP on any person that is NOT a CE! 68 FR 18898 (What about your business associates; are your BAs required to indemnify you for liability imposed on YOU by CMS as a result of the BA's acts/omissions?)

How do they Collect Penalties?

- Penalties are recoverable:
  - in a civil action in U.S. District Court (all collateral issues are estopped if they could have been raised by respondent below)
  - By Offset from "any sum owed … by the United States or a State agency." (this includes Medicare and Medicaid payments, and tax refunds!)
  - If you don't defend the penalties, they WILL collect them.



Can You Settle A HIPAA Case?

- Yes-DHHS can "settle any case or … compromise any penalty during the process"
- OCR has indicated that it favors settlement and that litigation is a "last resort).
- You may want to request a hearing as part of your settlement strategy; at the least, collection of the fines will be stayed pending the outcome of the appeal.

HIPAA Hearings

- Time is OF THE ESSENSE: 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."
- Time Period: Sixty (60) days after notice of the proposed penalty determination is received by the respondent.
  - Receipt date is "presumed" to be 5 days after the date of the notice. This is a rebuttable presumption, however.

HIPAA Hearings-Con't

- Hearing is on the record. There WILL be a written record made. Be prepared for ANYTHING you say (or is said on your behalf) to be used against you by the Government at some point.
- HHS party will be "OCR and/or CMS". If you don't name the correct party in your hearing request, and the time for filing the request passes, your right to a hearing may be abrogated. Get the caption correct!
- Discovery is "limited." (Document production, essentially) Depositions/Interrogatories are specifically prohibited. Base your strategy accordingly.

HIPAA Hearings-Con't.

- Decision of the ALJ is the decision of DHHS (contrary to many state systems, where an ALJ's decision can be adopted, modified or rejected by the head of the administrative agency)
- The CE MAY request judicial review of final penalty decisions (i.e., appeal to U.S. District Court)
- The CE may request a stay of penalty collection pending judicial review. (file federal appeal papers with ALJ; stay automatically granted until ALJ rules on request)

What to do BEFORE the Investigation?
5 Easy Steps to Avoid Investigations

- Step 1: Do your homework.
  - Develop, implement and document 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

- Tips to prove that you "did your homework":
  - Train your staff. Use care when developing training materials.
  - Maintain employee training time records and training materials used (Written Post-Tests STRONGLY Recommended)
  - Include the latest OCR HIPAA guidance in your training materials (http://www.cms.hhs.gov/hipaa/hipaa2/education/infoserie/)
  - Show your employees the online enforcement video from **OCR**, (http://www.ehcca.com/streaming/index.html)
  - How can OCR say that you didn't do it right, if you train your employees to do what OCR says to do?

What to do BEFORE the Investigation-Continued

- Step 2: Audit the Plan's Internal Functions
  - 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

- Step 3: Externally Audit Your Plan

A) Establish a Published Audit Plan

- What do you want to audit EVERY year
- What do you want to focus on THIS year
- Define known goals for your employees regarding known audit targets

B) Establish a Confidential Audit Plan

- Conduct "Mock" investigations yearly
- Simulate an irate patient seeking someone's head over a perceived privacy issue
- Choose "Moving" Confidential Audit Targets

What to do BEFORE the Investigation-Continued

- Step 4-Be Prepared, and Be Flexible (forewarned is forearmed)
  - Watch the Message Boards; see who is complaining about what
  - Watch the "official" HIPAA FAQs; they are a great window into OCR's enforcement priorities. As new FAQ's are added, revise your HIPAA compliance plan and your audit plan accordingly
  - Watch the news reports; don't perpetuate policies that have created bad press for "the other guy"

What to do BEFORE the Investigation-Continued

- Step 5: Make plans to move ahead
  - Derive Statistical Values from your audits
  - Show improvement OR plan to improve where you didn't
  - REPORT your progress to your governing body (don't be a target for investigative reporters looking for "cover-ups"
  - EXIT INTERVIEWS-A good opportunity to learn about what's NOT getting done

What to do BEFORE the Investigation-Continued

Practical Tips

- Integrate HIPAA compliance with usual business operations
  - 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!).
- 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!)

What to do BEFORE the Investigation-Continued

GET GOOD HELP!!!!

These are VERY complex regulations. The Security Rule alone can take a year off of your life, so GET AND RELY ON THE WRITTEN ADVICE OF COUNSEL AND 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!!!!!!!!!!!!!!!!!!!

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
www.hoaglandlongo.com
www.healthlawnj.com