Responding to a HIPAA Investigation: A Primer for Covered Entities

Marc D. Goldstone, Esq.
Partner
Hoagland, Longo, Moran, Dunst & Doukas, LLP
40 Paterson Street
P.O. Box 480
New Brunswick, NJ 08903
732-545-4717
732-545-4579 FAX
E-Mail: MGoldstone@HoaglandLongo.com
WWW.HoaglandLongo.com
WWW.HealthLawNJ.com

On April 14, 2003, HIPAA's Final Privacy Rule became effective. As a practical matter, healthcare providers, health plans and healthcare information clearinghouses that transmit certain electronic transactions (collectively, "covered entities", or "CEs") have had more than two years notice to implement their HIPAA compliance plans, so as to ensure adherence to the Privacy Rule's requirements. However, as the "rubber meets the road" there are sure to be undiscovered gaps in privacy practices; those gaps could be the basis for a government investigation into a covered entity's HIPAA procedures.

Development of an investigation response policy is one key to minimizing a CE's liability for HIPAA violations. The Office of Civil Rights ("OCR") of the U.S. Department of Health and Human Services has noted that:

> 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 …. OCR will seek to resolve matters by informal means before issuing findings of non-compliance. 68 FR 18897

Based on this, it appears as if the focus of the civil HIPAA enforcers will be to ensure compliance through assistance to covered entities; not through threats of legal action (at least, during the initial phases of an investigation). Given this stance, it would seem foolish for a CE not to work with OCR to some extent, if OCR comes to a CE's place of business with an official inquiry. Why skip negotiation and go straight to punishment?

So, what should a covered entity do if a government official "drops by" their offices one day for an official HIPAA chat? Hopefully, this article will provide a general framework by which an agency may guide its conduct so as not to create any additional liability for themselves when interacting with the government's HIPAA enforcers.

Step 1: Don't Panic. Really. It's important to keep calm when the investigators are at your door. The reason for this is simple-prosecutors "like" nervous interviewees. They like them so much that they oftentimes invite them back to the home office for a more in-depth discussion. Each covered entity should choose a liaison for investigations; that liaison should be someone that has a cool demeanor under pressure. If a covered entity's key executive does not possess this trait, they should recognize that fact and select another manager or employee to serve in this key position. The investigation liaison serves as the covered entity's "face" during the investigation; make sure it is a good one.

Step 2: Expect the Unexpected. Remember-Anyone may file a complaint with OCR; the complainant need not notify the CE before filing a complaint. Technically, complaints must be filed within 180 days of when complainant knew or should have known of the violation. Beware, however, that DHHS can extend this time period for "good cause shown". While OCR "will generally" give notice before requesting access to a CE's books and records, they are not required to do so! 65 FR 82602. Thus, a CE's compliance staff should be ready to respond to an investigation "out of the blue." It might be prudent to hold an "investigation" drill periodically, to ensure readiness.

Step 3: Phone Home. Each covered entity should have a "phone tree" that should be activated whenever an investigation occurs. The designated communicator should call:

- Your Attorneys (HIPAA counsel AND local counsel, if they aren't the same)
- Your Executive Management
- Your Privacy Officer
- Your Security Officer
- Your Compliance Officer
- Your Health Information Management Department/Custodian of Records

Everyone on this list needs to know that "the wolf is at the door". Everyone also needs to hear it from the horse's mouth; the only thing worse than not notifying these individuals in a timely manner is letting them hear it from the "grapevine." It would probably go something like this: Original Communication: "OCR is here to ask questions about our NPP acknowledgement." Grapevine Gossip: "OJ came by and acknowledged that we don't know anything about HIPAA". It's best if you immediately assign someone to make these calls (as part of a well-crafted "responding to investigations" policy that should apply to ALL official inquiries, not just HIPAA) OUT of sight (and hearing) of the investigators; you'll likely be too busy doing other things, and you really don't want to make the calls in front of them.

Step 4: Know What's in Store. Forewarned is Forearmed. HIPAA's privacy requirements that can be the source of civil monetary penalties are enforced by OCR. We know that enforcement activities will include:

- working with covered entities to secure *voluntary compliance* through the provision of technical assistance and other means;

- responding to questions regarding the regulation and providing interpretations and guidance;

- responding to state requests for exception determinations;

- investigating complaints and conducting compliance reviews;

- where voluntary compliance cannot be achieved, **seeking civil monetary penalties and making referrals for criminal prosecution**

How do we know this? Because the government published these comments in the Federal Register.

It's also important to know where enforcement initiatives will originate from. OCR noted that "[t]he [investigation] 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. "Complaint-driven" means that unhappy patients, disgruntled employees, former employees, competitors and others with an ax to grind will likely initiate HIPAA investigations.

Step 5: What to do when OCR arrives at your door. Here are some of the things that I recommend:

- Cooperate (but cautiously!) Ask for the official government agency issued identification of the investigators (TIP #1-Business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. (TIP #2-if they can't produce acceptable I.D., call your attorney immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D.-but BE SURE that you've made appropriate requests for I.D. and that they've been unreasonably refused before you do.) (TIP #3-I would have at least one, if not two witnesses available to testify as to your requests and their response if you are going to go down this route).

- Ask for the name and telephone number of the lead investigator's supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering "hard feelings." Under NO circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators. If you can obtain this information, your attorney will thank you for it, because it will prove an invaluable "short-cut" to obtaining information about the investigation, and may potentially clear the way to a settlement in short order, if advisable (thus, reducing your legal fees).

- Be sure to determine if there are any law enforcement personnel present (i.e., FBI, US Attorney investigators, State Prosecutor investigators, etc.). Again, this is information that will be invaluable to your attorney (to help him/her make a determination as to the gravity of the investigation; if law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation). Generally, guns strapped to hips are a good indicator of the presence of law enforcement personnel; but, if in doubt, ask.

- DO permit the investigators to have access to protected health information ("PHI"), in accordance with your notice of privacy practices ("NPP"), and Federal and State law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them, if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Again, ask them to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records (TIP #4-Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. Two witnesses are even better! All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.)

- Send your staff employees elsewhere, if possible. There is absolutely no requirement that you provide witnesses to be questioned by the government during the initial phases of the investigation; likewise, there is no need for you to connect the investigators with any disgruntled employees. If necessary, give your employees the rest of the day off; but do whatever you have to do to send them away and keep them away. Definitely consider it a game of "keep away" that you need to win. Unless the investigators subpoena your employees (which they probably won't do until after the initial visit) you likely have no Federal duty to line up your employees for questioning at this point (although, State laws may vary on this one; check with your local counsel for more specific info.). Do NOT instruct your employees to hide or conceal facts, or otherwise mislead investigators, though, once they are face to face with OCR-that's called obstruction of justice, and it is a crime in and of itself.

- Ask the investigators for documents related to the investigation; for example, request—

  - copies of any search warrants and/or entry and inspection orders

  - copies of any complaints

  - a list of patients they are interested in

  - 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 documents/items seized (if any).

- Don't leave the investigators alone, if possible. Assign someone to "assist" each investigator present.

- Don't be TOO solicitous—

  - Don't offer food (coffee, if already prepared, and water, if already available, if probably ok; don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch)

  - Don't get "chatty." Although OCR has indicated they are here to help, these people aren't your friends; only tell them what you are required by law to tell them; always defer to the advice of counsel if you are unsure. Don't be uncooperative; don't exhibit a poor attitude; do answer direct questions fully and to the best of your ability. Don't offer opinions; don't talk about your competitors; especially don't complaint about the burdens associated with HIPAA compliance OR the government.

- Notify your State Practice Association, if you feel comfortable, under the "Golden Rule" theory, to help "spread the word" about local enforcement activity, as well as to obtain their assistance. Most State Associations have a government relations coordinator who has contacts that may be valuable to a covered entity under investigation; the only way to access those contacts is to make the call.

Step 6: What CAN they do to you? It's important to know the potential consequences of a HIPAA investigation, before deciding what your response will be. If OCR determines that a CE has committed a HIPAA civil violation, they will:

- Inform the CE (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 the violation is egregious enough to constitute a crime, DHHS "shall impose"

- Criminal Fines: up to $50,000 and/or 1 year in jail

- If the crime involves obtaining, using and/or disclosing PHI under false pretenses, the penalty can include a fine of up to $100,000 and/or 5 years in jail

- If the crime involves the intent to sell, transfer, or use IIHI for commercial advantage, personal gain, or malicious harm, the penalty can include a fine of up to $250,000, and/or 10 years in jail

Remember that OCR enforces civil violations of the Privacy Rule; criminal issues are referred to OIG and the Department of Justice.

If no violation is found, OCR will inform the CE and the complainant, if any (nothing says this notification must be in writing).

Can a CE be excluded from Federal Healthcare programs based on a HIPAA violation? Is a HIPAA violation also a violation of the Medicare Conditions of Participation? DHHS has "not yet addressed" it; however, DHHS did "note that Medicare conditions of participation require participating providers to have procedures for ensuring the confidentiality of patient records". 65 FR 82605.

Step 7: Know DHHS' Limitations. Every CE should be aware that:

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

- 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).

- 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).

- 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).

- 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.

- 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).

- DHHS CANNOT impose a HIPAA CMP on any person that is NOT a CE! 68 FR 18898

Step 8: Know When to Hold 'em, and Know When to Fold 'em. Sometimes, discretion is the better part of valor, and it makes sense to settle charges of a HIPAA violations. There is a specific process to settle a case, though, and it is important to follow the procedures to the letter.

- 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.

- 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.

- Hearings are on the record. 45 CFR Part 160.530(a); 560.

- The 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) (This is contrary to many state administrative law 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; the stay is automatically granted until ALJ rules on the request).

Step 9: What to do BEFORE the investigation. Two words-Be Prepared!

- Implement your HIPAA Compliance Plan to the greatest extent; if you take reasonable and scalable steps to comply, you can make all of your "incidental disclosures" permissible pursuant to the Final Privacy Rule, and thus, they will not constitute HIPAA violations.

- Document the steps that you took to implement your plan; HIPAA committee minutes (if you have a HIPAA compliance committee) should be maintained 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.

- Periodically examine reports to your Privacy Office/HIPAA Hotline (suggest semi-annually or more).

    - Investigate ALL reports and conclude ALL investigations with WRITTEN documentation.

    - 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!)

- Train, educate, explain, and then train some more.

- Maintain employee training time records, training funds expended, and training materials used (TIP #5-Make sure each employee takes and passes a HIPAA training post-test. If they fail, re-train them and test them again).

- Create a "Culture of Privacy" (which probably already exists at most healthcare facilities)

- Read the latest OCR HIPAA implementation and enforcement guidance at: http://www.cms.hhs.gov/hipaa/hipaa2/education/infoserie/

- Watch the online enforcement video from OCR, at http://www.ehcca.com/streaming/index.html. This is 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!).

- 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.

It's important to remember that OCR is a relatively "new animal" to those of us in the healthcare field. We have some experience with OIG investigations, but we're just not sure how OCR will treat us. A strong, effective compliance plan, and a well-crafted response to investigations policy will be your best tools to survive a HIPAA investigation and not get trampled by the HIPAA HIPPOs (Health Information Protection Police Officers).