Real World Tips and Tricks to Help You Implement, Run and Audit Your HIPAA Compliance Plan

Marc D. Goldstone
Hoagland, Longo, Moran, Dunst & Doukas, LLP
New Brunswick, NJ
732.545.4717
Mgoldstone@hoaglandlongo.com

Kirk J. Nahra
Wiley Rein & Fielding LLP
Washington, D.C.
202.719.7335
KNahra@WRF.com

Introduction

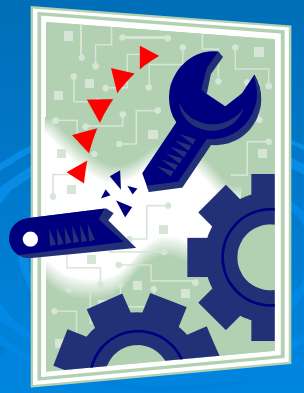
- We are now two years into the HIPAA Privacy Era
- Ongoing Changes, due to the Security Rule and developments related to the Privacy Rule
- Looking at the key aspects of ongoing monitoring and auditing – for both your own HIPAA plan and those of your vendors

Topics for discussion

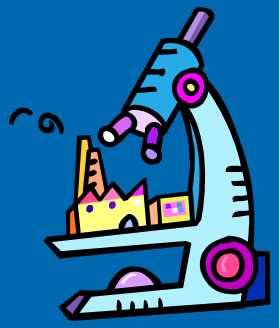
- Ongoing implementation challenges
  - HIPAA is still pretty NEW; we don't even know what we DON'T KNOW yet.
- Auditing your own program
  - If your plan is a "book on a shelf" then you don't have a plan to begin with
- Dealing with your vendors
  - Nobody is horizontally or vertically integrated enough NOT to need a vendor of one sort of another (even if the vendor is simply a janitor). You need to ensure that your vendor relationships don't create HIPAA liability.

Some Implementation Challenges

- Contracting issues with business associates
  - Who is a BA? When is a "business associate" NOT a "Business Associate"?
- Individual rights
  - When are disclosures REQUIRED?
- Oversight Agency Authority
  - What's your plan when your regulators want your PHI?
- Mitigation
  - You WILL have an accident at some point. What do you plan to do when that occurs?
  - What about "Bad Actors"?
- What else?



Why Audit?



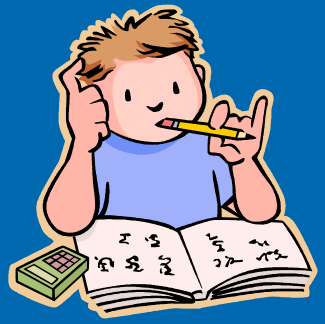
- Compliance plans must be “effective” in order for the Government to consider them a “mitigating” factor in enforcement actions
  - Written audit results are a great way to prove your plan is “effective”; especially if you made material changes to operations or to the plan in response to data gathered as the result of an audit!
- Compliance plans don’t come with an “auto-pilot”; if you don’t audit them, you don’t know if they are working (and why spend $$ on something that isn’t “effective”, doesn’t work, and doesn’t get you a reduced penalty?)

What to do BEFORE the Investigation?

5 Easy Steps to Avoid Investigations

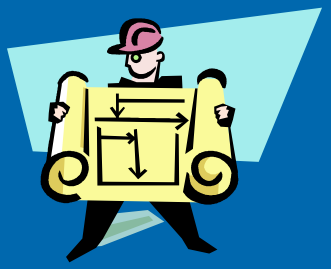
- Step 1: Do your homework.
  - Develop, implement and document your HIPAA Compliance Plan to the greatest extent possible (gain HPBs [HIPAA Brownie Points]; make all of your "incidental disclosures" permissible pursuant to the Final Privacy Rule).
  - Document the steps that you took to implement your 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. AVOID "CANNED/GENERIC" MATERIALS.
  - Maintain employee training time records, and copies of 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



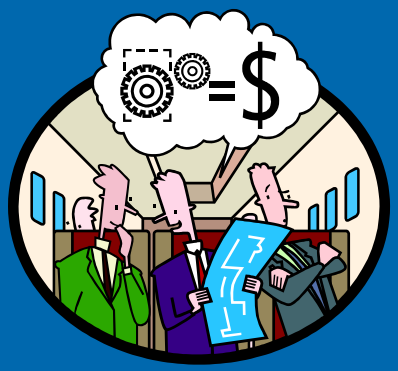
- Step 2: Audit the Plan's Internal Functions
  - Periodically examine reports to your Privacy Office/HIPAA Hotline (suggest semi-annually or more)
    - Investigate ALL reports and conclude ALL investigations with WRITTEN (VDTM-Vertical Dead Tree Media) documentation (sample form attached)
    - Trend 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!!!!

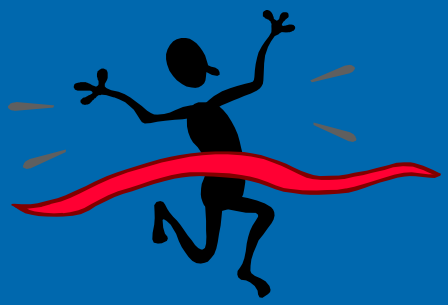
These are VERY complex regulations. The Security Rule alone can take a year off of your life, so GET AND RELY ON THE WRITTEN ADVICE OF COUNSEL AND QUALIFIED CONSULTANTS!!!! (at best, they'll be right; at worst, you can be indemnified by their professional liability policies!) Due diligence is important in developing an effective HIPAA compliance plan.

Help...

Challenges with Vendors

- Vendor issues
- Identifying vendors who have high risk activities (based on sensitivity, volume, client-facing, etc)
- Off-shoring issues – heightened sensitivity (but is this really any different?)
- Oversight on an ongoing basis
- Due Diligence on the front end
- Contractual requirements – how much is enough and too much

Conclusions



- We have NOT yet discovered ALL of the HIPAA implementation challenges; when you find a new one, be sure to document how you dealt with it
- Auditing your plan makes it effective (or more effective); it's like putting high octane gas in an expensive sports car. A sports car with no gas is just a pricey paperweight. A compliance plan with no audit plan is just an expensive pile of VDTM.
- Vendors serve YOU; not the other way around. If they won't cooperate in your compliance efforts, you need a GOOD reason (more VDTM) why you continue to retain them.

Thanks!

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

Any Questions?

Marc D. Goldstone
Hoagland, Longo, Moran,
Dunst & Doukas, LLP
New Brunswick, NJ
732.545.4717
Mgoldstone@hoaglandlongo.com

Kirk J. Nahra
Wiley Rein & Fielding LLP
Washington, D.C.
202.719.7335
KNahra@WRF.com