HIPAA Summit Presentation Practical Tips to Help AVOID Enforcement

Marc D. Goldstone, Esq.

Disclaimers

- Nothing I say is the position (official or otherwise) of the Tenet Health System, or any Tenet Hospital. The words, thoughts, and expressions are solely my own.
- Your Mileage May Vary
- Priced Higher in Alaska and Hawaii
- If Symptoms Persist For More Than 24 Hours, Seek Immediate Medical Attention …

What Are We Going To Do Today?

- We'll go over some of the biggest problems I'm seeing with CEs trying to comply with the (relatively) Old Privacy Rule, the (relatively) New Security Rule, and the (still newer) Enforcement Rule.
- In each instance, we'll give you a "*Take Away*" to help you focus on HIPAA compliance AS A MEANS TO AVOID ENFORCEMENT
- Finally, we'll talk about what may be "coming next"

What Does the Privacy Rule Require?

- All covered entities must establish policies and procedures to ensure compliance with the Final Privacy Rule
- Under the Privacy Rule, a CE CANNOT "USE" or "DISCLOSE" PHI unless specifically authorized by the rule, OR authorized by a STRICTER state law.
- *Take Away: : This is actually a pretty easy rule to comply with (relatively speaking); it boils down to 5 steps, really:*
  - *Keep private stuff private*
  - *Write down how you plan to do that*
  - *Give your privacy policy to patients*
  - *Train your staff, and*
  - *Keep records of what you did to comply.*
  - ***Do you have those written records on file? Most don't!***

What Does the Security Rule Require?

- CEs must "[m]aintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of the protected health information and to protect against reasonably anticipated threats or hazards to the security and integrity of the information, use or disclosure of this information."
- OK, so this one's not as easy as the Privacy Rule

What That Means "In English"

- Covered Entities must:
  - Use their best efforts (or at least document that they gave it a really valiant try) …
  - to apply the best safeguards (or at least an affordable method that provides reasonably strong protection) …
  - to prevent the unauthorized modification or alteration of electronic form PHI (E-PHI) in their possession, and …
  - protect E-PHI from those who do not have a right to possess or view it, and …
  - protect E-PHI from computer viruses, worms, hackers, packet sniffers, disgruntled employees, etc., and also …
  - protect E-PHI from hazards such as lightning, floods, fire, etc.
- I said it would be "in English"; I didn't say it would be brief.
- *Take Away: The ESSENCE of HIPAA Security Rule compliance is responding appropriately to a changing world. If you create a HIPAA compliance plan and don't have annual updates on file, you will almost certainly NOT be in compliance. You need to have a PLAN to do the updates (and document your efforts), or you probably won't.*

Is There A Roadmap?

- The Security Rule permits each CE to review their own internal strengths and weaknesses, and then implement appropriate and reasonable action to comply with the Rule's requirements, based on the CE's size, needs, budget, etc.
- The Security Rule DOES require that CEs maintain detailed WRITTEN records of compliance.
- Thus, each CE sows the seeds of their own success or failure regarding the Security Rule, and, more disconcertingly, CE's must provide the "smoking gun" proving their failure to comply with the Security Rule to the Government, if asked!
- *Take Away: A GOOD HIPAA COMPLIANCE PLAN CAN SAVE YOUR BUTT; A BAD ONE CAN BURN YOU. MAKE SURE YOURS IS GOOD, AND MAKE SURE IT STAYS GOOD VIA REGULAR UPDATES!!!*

What to write down for the Security Rule?

- Have you implemented a HIPAA compliance committee? Does the committee have input from administration, technical services, and professional care providers?
- Have you reviewed the final Security Rule? (You can download it from the CMS website, www.CMS.gov).
- Have you conducted a risk analysis? It should look at all of your electronic data storage, use, reproduction and transmission systems to see what risks to electronic protected health information (e-PHI) exist.
- Have you implemented risk management policies and practices to reduce the risks to your e-PHI? You should have fixed the risks revealed by the risk analysis.
- Have you established a written HIPAA Security Rule compliance plan? Is it tailored to your facility/practice? Does it reflect what you actually do, on a day-to-day basis? Does it reflect any "cost/benefit" and/or "addressability reasonableness" decisions you made, and the detailed reasons why you made them? Does it require that you update it, in writing, annually? Does it require that you audit it regularly, and keep the audit results, in writing? Does it require you to make changes based on the audit results and/or trends thereof? It should!
- Have you published a sanction policy? You should have told your employees, in writing, that security violations are treated seriously by your company.
- Have you published a procedure to regularly review information system activity? You should have an ongoing mechanism to identify new breaches or potential risks. You should perform this review no less than annually, and document the results, and your responses to the information discovered.
- Have you assigned an individual responsible for security? It is highly unlikely that a privacy officer is also qualified to be the security officer. Appoint a security officer who is qualified for the job by training, education and/or experience.
- Have you trained your employees to keep private health information private, and to protect the security of your e-PHI? Do you require your employees to sign confidentiality agreements concerning your PHI and e-PHI?
- Have you established procedures to establish clearance for members of your workforce to have access to e-PHI? You should know which employees have and do not have access to systems that store, maintain or transfer health data. You should have decided who will get a password to use systems that can access e-PHI, and that decision should be made based on each employee's REAL need for access to e-PHI in connection with their job.
- Have you implemented termination procedures for workforce members who leave your employ? Did you take back the keys and turn off passwords immediately before or at the moment of after termination? Do you have a written policy regarding what security steps to take in connection with the termination of an employee who was cleared for access to e-PHI?
- Have you implemented procedures for the supervision of workforce members who access e-PHI? Have you taught your supervisors how to supervise employees for compliance with the security rule?
- Have you implemented a procedure for reviewing and implementing periodic security updates? Do you buy and install new and upgraded security (including virus protection and firewall) software and/or hardware when available/appropriate?
- Have you implemented a means to monitor log-in attempts? Can a hacker attempt to gain access unlimited times, or will the system shut down after a number of attempts? Will somebody know about it? Will the system keep a record of who "knocked" at your "electronic door"?
- Have you implemented procedures for password management? You should require people to keep their passwords secret, not to share them with other employees or disclose them to others, change them frequently, and pick ones that are hard to guess.
- Have you established a means for reporting security incidents, including unsuccessful attempts to breach your security? You should have specified the process by which your employees report security incidents (preferably immediately, and in writing) and how you respond to them. You should require your security officer to keep written records of your responses to security incidents.

What Else?

- Have you established a contingency operations plan? If a particular system is interrupted, will you have another way to make critical e-PHI available to users?
- Have you established a data backup plan? Do you regularly back up your data in case some or all of it is lost, and do you keep the backup copies somewhere other than your office (preferably a really safe location)?
- Have you prepared a disaster recovery plan? Does your staff know how to go about getting your electronic systems up and running if you have a fire, flood, or other catastrophic loss of electronic systems?
- Have you established procedures for the continuation of business processes while operating in emergency mode? Can your doctors and other people who rely on your data keep working in a contingency situation?
- Have you implemented procedures for the periodic testing and revision of your contingency plans? Do you have disaster drills that show that your disaster recovery plan, continuation of business processes contingency plan, and data backup plans actually work?
- Have you assessed all of your applications and data to determine the criticality of each in relation to all others? Do you know what you need to restore first, and have you prioritized which systems need to be brought up first, in the event of a catastrophe?
- Have you performed an evaluation of your technical and non-technical security measures protecting electronic protected health information? After you implement all your security steps, have you thought about whether what you've done is the right fit for your organization? Do you check after each material business change to see if you need to do things differently?
- Have you updated your business associate contracts (with specific E-PHI security provisions) with each business partner? Your existing privacy rule agreements need new security rule sections; agreements executed on or after 4/20/05 need to contain privacy AND security provisions.
- Have you established rules regarding your employees' physical access to systems that can access e-PHI, and the areas where such systems are located?
- Have you established policies concerning the use, reuse, and disposal of systems and storage devices that contain e-PHI?
- Have you established a policy on dealing with inappropriate access to facilities and/or locations that contain systems that can access e-PHI?
- Have you mitigated physical risks to your computer systems (i.e., water damage from sprinkler systems, etc.)
- Have you developed a policy for ensuring the destruction of e-PHI when it is no longer needed? Does that policy require more than merely "deleting" the information from a hard drive? It should!
- Have you instituted entity authentication policies, if appropriate? Such authentication policies might require the use of both a password and a "biometric" identifies, such as a fingerprint, in order to access e-PHI.
- Have you instituted policies and procedures to protect your system from intruders, and from individuals (including employees) who might make unauthorized changes to, or destroy your e-PHI?
- Have you instituted policies and procedures, such as encryption, to protect your e-PHI when it is transmitted from one location to another?

That's All?

- So then, that's all there is to do, right? Fill out a checklist?
- Not really. A lot of what is already in place at most CEs concerning the security of electronic data may be fine for Security Rule compliance, but it is unlikely that any CE is 100% compliant without ANY "tweaking" at all.
  - For instance, most CE's don't have a formal risk assessment document. Checking "yes" on the checklist in that case is a recipe for disaster.
- *Take Away: Remember, a checklist is NOT compliance in and of itself. Ever look at the "backup", as the accountants like to say?*

"Shall Do" or "May Do"?

- The Rule establishes that each Specification is either *REQUIRED* or *ADDRESSABLE.*
- Required Specifications are, well… required. Gotta comply.
- Addressable Specifications are those that are not likely to be an issue with every covered entity, but must be addressed if one or more apply to a CE's particular circumstances. You do HAVE to write down what you decided to do, and WHY.
- It's a little like Purgatory-your Security Rule compliance plan can place you between Security "heaven" and "hell".
- *Take Away-whether or not a security specification needs to be addressed by your organization CHANGES as your organization changes. Therefore, you need to periodically assess your HIPAA compliance plan, and your organization's needs and abilities, and write down any changes that you make, ESPECIALLY concerning ADDRESSABILITY. Being in compliance "last year" will not help you if the government decides that you're not in compliance "NOW".*

The Single Most Common Security Rule Problem I've Seen To Date

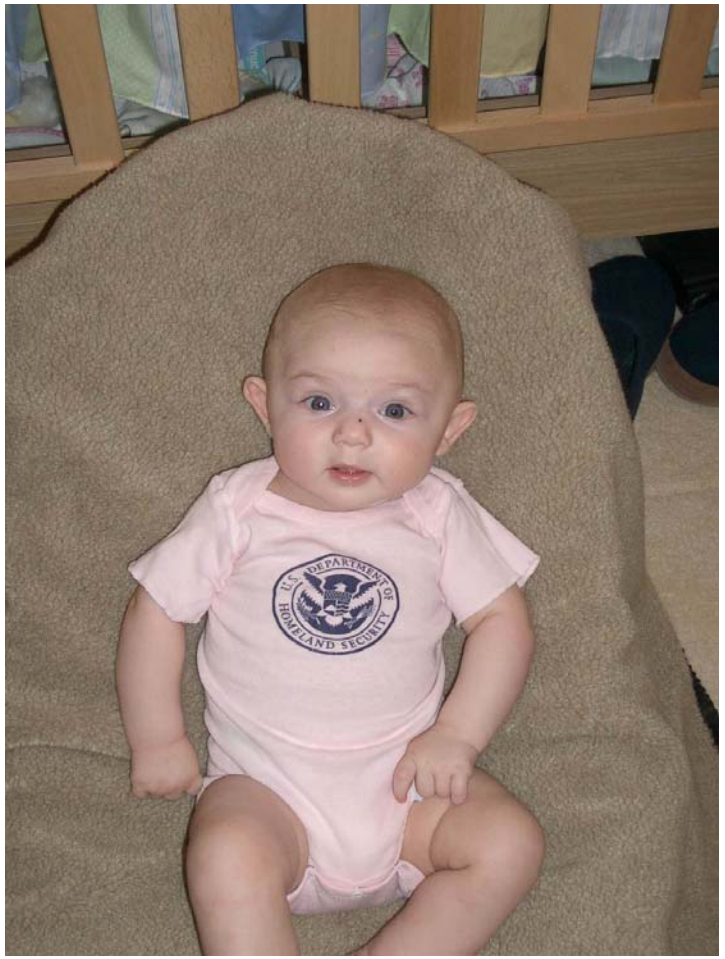
- The Security Rule requires CEs to conduct and document a Risk Analysis (a thorough assessment of the potential risks and vulnerabilities to the security of their protected health information) and to have written Risk Management procedures in place
- ***Take Away-In almost EVERY investigation involving security rule violations, the government will ask you to produce your baseline audit and your risk management policy. You need to have both, in writing, and BOTH need to be periodically updated to reflect changes in your organization AND changing risks to your data. If you don't have them, you're NOT in compliance.***

More Common Problems

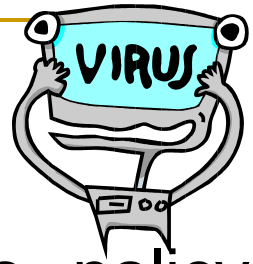
- CE's must implement a "Sanction Policy", to take corrective actions against employees who fail to comply with the CE's privacy and security policies and procedures. Corrective actions and sanctions should be graduated according to the severity of the breach.
  - *Take Away: CEs tend to just "lump in" HIPAA violations with their usual progressive discipline policy. If an employee receives the same discipline for a privacy or security breach as they do for being 7 minutes late, the government may not believe that the CE has truly implemented an effective HIPAA compliance plan.*

Common Problems-Con't

- CE's must have a policy in place to ensure the appointment of an appropriately qualified and trained Security Officer (and someone actually has to get appointed!)
  - *Take Away-There are dozens of certifications in the I.T. world; do some "due diligence" to be sure that the Security Officer has the experience and qualifications to do the job, no matter how much "alphabet soup" he or she lays claim to. It is VERY unlikely that your Privacy Officer is ALSO qualified to be your Security Officer, and OCR knows this. However, many CEs don't seem to be aware of this fact!*



Common Problems-Con't.



Security Reminders: The CE must have a policy regularly to remind each member of the workforce of the CE's security policies.

- *Take Away: CEs should obtain each employee's signature to prove that they received the periodic (i.e., ANNUAL) written reminder. Security post-test results are excellent documentation.*

- Protection from Malicious Software: Each CE must establish procedures to protect their systems from malicious software.

- *Take Away:3 words-Anti Virus Program. Make sure it's updated regularly. Keep records to prove that you added updates as they became available.*

Common Problems-Con't.

Media Disposal: A CE must implement procedures to assure that E-PHI does not remain on discarded computers or components.

- *Take Away-Think Sledgehammer. Really. Physical destruction is good. If you just "throw them away", someone will find them, and the e-PHI on the hard drives will be at risk for inappropriate use/disclosure!*

- Media Re-Use: A CE must establish a procedure to "scrub" E-PHI from media when the media is to be re-issued or decommissioned.

- *Take Away-Simply deleting data/formatting a hard drive DOES NOT render the E-PHI on that device unrecoverable; it's just harder to access. Before the media is reused, the CE must have a procedure to "shred" or otherwise eradicate the data on it. E-PHI CAN "LIVE" FOREVER UNLESS YOU AFFFIRMATIVELY KILL IT!!!!!!!!!!*

Enforcement Rule Issues

- Violation? New rule clarifies that the Enforcement Rule applies to “Acts” AND “Omissions”
- “a violation occurs when a covered entity fails to take an action required by a HIPAA rule, as well as when a covered entity takes an action prohibited by a HIPAA rule” 70 FR 20229
- *Take Away: Your compliance plan should contemplate what happens if someone “fails to act”. That’s VERY DIFFERENT than disciplining someone for affirmatively disclosing PHI.*

Enforcement Rule Issues-Con't

- New rule BROADENS scope of the Enforcement Rule
- the term ``administrative simplification provision'' in Sec. 160.302 means **any requirement or prohibition established by the HIPAA provisions or HIPAA rules**: ``* * * any requirement or prohibition established by: (1) 42 U.S.C. 1320d-1320d4, 1320d-7, and 1320d-8; (2) Section 264 of Pub. L. 104-191; or (3) This subchapter.'' 70 FR 20228.
- *Take Away: Many HIPAA Compliance Plans Created from "off the shelf" products likely do NOT take into account this expanded enforcement mandate; you may need to make changes!.*

HIPAA Hearings-Issues

- Testimony and other evidence obtained in an investigational inquiry may be used by HHS in any of its activities and may be used or offered into evidence in ANY administrative or judicial proceeding (La. Clinic Case).
- *Take Away: You may be handicapped in your defense of a HIPAA complaint due to underlying state law interests; be careful who is permitted to say what to whom in the course of an investigation. You can find yourself settling a 25 Thousand Dollar HIPAA complaint, but setting up a multi-million dollar verdict in State Court!*

HIPAA Hearings-Issues Con't

- When a penalty proposed by the Secretary becomes final, the Secretary notifies certain specified appropriate State or local agencies, and "the public generally." 70 FR 20240
- So, in addition to "the appropriate State or local medical or professional organization, the appropriate State agency or agencies administering or supervising the administration of State health care programs, the appropriate utilization and quality control peer review organization, and the appropriate State or local licensing agency or organization, now EVERYONE will know.
- Posting to an HHS Web site and/or the periodic publication of a notice in the Federal Register are among the methods which the Secretary is considering using. Id.
- *Take Away: If your settlement agreement is made public, it may not be as good a deal as you otherwise thought, so consider the effect of publication on your business before making a settlement decision.*

What's Coming Next

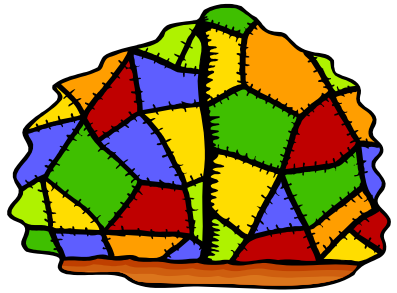
- Phishing-Can you rely on your employees' "common sense"? If you don't train them to spot and avoid common "phishing" scams, are you HIPAA-liable?

Coming Next-Con't.

- Vicarious Liability for Bad Actor Employees-DOJ has recently taken the position that ONLY CEs can be charged with HIPAA crimes. If an employee (who is NOT a CE) commits a HIPAA crime, how do you avoid becoming a target of the prosecutors?

© Scott Adams, Inc./Dist. by UFS, Inc.

Coming Next-Con't.



- Patch Management-when a vendor releases "fixes" for software, how does a CE manage the process of authenticating and installing the "patches."
- If you don't install a patch, are you guilty of a *per se* HIPAA violation?
- If you are using software that continually needs patches in order to remain "secure" (think Windows/I.E.), have you made a choice to ignore the Security Rule?

Any Questions?

- Thanks for your kind attention!
- Follow-up questions/inquiries to:
  - Marc.Goldstone@Tenethealth.com
  - Telephone: 732-545-4717