HIPAA Live: From Plan to Breach to Investigation to Resolution

Marc Goldstone
Senior Counsel
Tenet Health System
Ft. Lauderdale, FL
Marc.Goldstone@tenethealth.com

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

HIPAA Summit
(September 2006)

You had a bad day

- It's a bad day to be a privacy officer.
- You walk into your office first thing in the morning, and have a voicemail. It says that one of your biggest contractors, a consulting firm that has been analyzing your billing and collection efforts, has lost a laptop containing all of your patient bills for the last two years.
- While you're digesting that, your HR director walks in. Seems one of your IT people stormed out of the office yesterday, after a simmering feud with his boss exploded, and there's been a huge number of e-mails sent from his desk to an unidentified external address, containing large volumes of patient medical records.
- So, what are you going to do?

First Step

Don’t Panic!!!!

This stuff is hard, but manageable. Try to plan out in advance how you’re going to handle these situations.

What we're going to cover

- The security breaches –
  - Mitigation issues – fixing the problem
  - Notification issues – to individuals, regulators, customers, etc.
  - Issues to watch out for
  - The differing legal standards
- Investigation issues
  - Dealing with an investigation
  - Who might be investigating and how they work

What's happening?

- Astonishing number of media reports about large and small security breaches
- Almost daily occurrences, affecting all industries
- Has led to state laws – in more than 35 states – about notification of individuals in the event of a security breach
- Likelihood of new federal legislation
- Driven by concerns about identity theft

Issues for the health care industry

- Health care industry has not been immune from identity theft issues - Eleven defendants were indicted on federal charges for allegedly conspiring to steal the identities of more than 100 patients at two medical practice groups and then using that information to steal at least $150,000 from the victims' bank accounts between 2000 and 2003.
- Some defendants were employees who improperly accessed patient medical records, then sold the information.
- Trend toward "apologies"; this may work in connection with medical errors; we're not so sure that it will be effective in connection with Security Breaches.

Mitigation

- Do I have an effective mitigation plan for privacy or security breaches?
- Major issue – tricky challenges when there is a high risk situation
- What are the standards of responsibility?
- Potential litigation over mitigation costs
- May have specific legal and contractual obligations
- Your compliance staff may urge an “apology”

Mitigation

- Mitigation involves:
  - Identifying the problem
  - Determining the cause of the problem
  - Evaluating any potential harm from the problem
  - Stopping the bleeding from the problem
  - Evaluating appropriate changes (if any)
  - Determining any other legally required steps (or appropriate business steps)
  - Does mitigation **require** notification to patients?

Intersection between HIPAA and state notice laws

- Security Incident-how do you determine IF you actually had one? Pings? Hacking?
- State notice laws
- Overlaps, under and over inclusive – some "security incidents" do not require notice under state laws, some situations require notice under state laws, but not HIPAA (employee data)

"Security Incident"

- HIPAA Definition – the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- If there is a security incident, what happens?
- Reporting to – covered entities (by business associates)? Regulators? Individuals?

Notification

- Must think about these issues now – after a breach, it may be too late
- Think about law, P.R., politics, etc.
- A very complicated practical issue
- Remember that notice doesn't get you out of a lawsuit about privacy or security harms – just out of violating the notice laws.
- Principal/agent issues

How “notification” works

- Defining the incident – what happened, what information was involved
- Was there any realistic harm of harm?
- What are your contractual obligations?
- What are your legal obligations?
- What is MORE harmful; getting in “front” of the issue, or getting caught “behind” the eight ball if someone else finds out that you DIDN’T disclose- this is truly a “fact sensitive” investigation.

Contract obligations

- Is this a HIPAA business associate situation, where there are notice obligations by the business associate based on a “security incident” – “security incident” means “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”
- Don’t forget about contractual indemnification, which may require ACTUAL notice in order to vest.

Contract Obligations (2)

- Identifying whether this standard is met – and whether your contract makes any modifications to this standard
- Are there other contract obligations? (timing, specifics, cooperation, etc)
- Notice here is to the client, not to any specific individuals

Legal obligations on notification

- Who does the law apply to? For Example:
  - "[a]ny person or business which conducts business in New York State, and that owns or licenses computerized data which includes private information."
- Typically applies to any company doing business in a state or where the residents of a state are affected.

What information?

- An individual's first name or first initial and last name in combination with any one of the following data elements, when either the name or the elements are not encrypted or redacted:
- i. social security number
- ii. drivers license number
- iii. Account number, credit/debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

What triggers notice?

- Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. (California)
- Unauthorized access and acquisition of unencrypted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur, or creates a material risk of consumer harm (North Carolina)

Notice to whom?

- "Owners" of data typically must provide notice to affected individuals
- Are there "indirect" notice obligations? – "[a]ny person or business that maintains computerized data that includes personal information that [they do] not own shall notify the owner or licensee of a breach."
- In most situations, a "covered entity will give notice directly, while a "business associate" will give notice to the covered entity.
- Clear exception of employment records, where any employer has direct notice obligations

Notice Complexities

- An opportunity to “point fingers”
- Other practical exceptions where a business associate (or other vendor) would provide notice directly?
- Risks to a business associate from notifying the customer (business and litigation)

Key Notice Issues

- What data?
- Encrypted?
- Electronic or other?
- What kind of notice standard in the relevant law(s)?
- What states are involved?
- Likelihood or risk of harm (remember, complying with the notice statute doesn't mean you won't get sued)
- Business environment?

Vendor issues

- Vendors
  - Overall oversight
  - Increasing standards focusing on ongoing monitoring
  - Involvement in security breaches
  - Audits
  - Increasing legal standards

Vendor control principles

- G-L-B standards (now applied to everyone) require companies to oversee service providers by due diligence and requiring contractual security standards
- HIPAA Security Rule assumes some oversight
- Major ongoing challenge to oversee and monitor vendor behavior
- Issues where there are security breaches
- Applies to most companies as both “principal” and “agent” (or vendor)

Investigation issues

- Who might investigate?
- How does HHS handle these investigations?
- How might others (FTC, State attorney generals) handle things differently
- Are there strategic concerns to notifications that may impact resultant investigations?
- What words should you NEVER, EVER utter to an investigator?

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

How Does 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 [Security] Rule and may provide technical assistance to help covered entities voluntarily comply"-"enforcement activities will focus on obtaining voluntary compliance through technical assistance."
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 [generally] be *complaint-driven* and consist of progressive steps that will provide opportunities to demonstrate compliance or submit a corrective action plan.

If OCR Knocks At Your Door

- Cooperate (but cautiously!) Ask for the official identification of the investigators (NOT business cards); write down their names, addresses, telephone and 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.)
- REMEMBER – In a security breach investigation, law enforcement may be a friend and an opponent

What Do You Have to Disclose?

- 162.502(a): A CE may NOT use or disclose PHI unless PERMITTED or REQUIRED by this section or by Subpart C (compliance and enforcement)
- 162.502(a)(2): Required disclosures are:
  - To the patient (524/528)
  - To the Secretary when required under Subpart C to determine compliance WITH THIS SUBPART (NO REFERENCE TO COMPLIANCE WITH OTHER LAWS!)

Disclosures for Law Enforcement Purposes?

- 164.512(a): MAY disclose if REQUIRED by law AND the request complies with and is limited to the requirements of the law
- CE must be compliant with:
  - 512(c)-abuse/neglect/violence
  - 512(e)-judicial/administrative proceedings
  - 512 (f)-law enforcement purposes (criminal subpoena, grand jury, info to locate a suspect, crime reports, location of victims, etc.
- Of course, there's always 164.512(d)-Health Oversight Activities (for oversight activities "authorized by law", including audits, criminal investigations, inspections, etc.)

Health Oversight Limitation

- 164.512(d)(2): The investigation MUST ARISE out of AND be DIRECTLY RELATED TO:
  - The receipt of health care
  - A claim for benefits related to health, OR
  - Qualifications of or receipt of public benefits or services where a patient's health is integral to the claim.

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)
- DO NOT DESTROY ANY PAPER OR ELECTRONIC RECORDS (INCLUDING HARD DRIVES); IF YOU TAKE REMEDIAL TECHNICAL MEASURES IN THE INTERIM, BE PREPARED TO DESCRIBE YOUR SYSTEMS AS THEY EXISTED AT THE TIME OF THE BREACH!

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 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

Violation of C.O.P?

- 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
- *Case Study-Are They Even Investigating HIPAA complaints, or is HIPAA merely a concern for the target of a wider investigation? Can you limit the use of your investigation-related disclosures?*

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

7. DHHS CANNOT impose a HIPAA CMP on any person that is NOT a CE! (Are your BAs required to indemnify you for liability imposed on your as a result of their acts/omissions?)
   - *Case Study-Are any of the Entities under investigation CEs? Are they BAs of a CE?*

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/Security 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 and Security” (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

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

What to do BEFORE the Investigation-Continued

- 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.

Breach Conclusions

- You will have breaches
- Consider HIPAA, state law and the rest of the universe
- Look at your legal obligations, and your appropriate responsibilities
- REMEMBER – Notice doesn't prevent you from getting sued
- Make sure you have fixed the problem
- Make sure it doesn't happen again