

# Breach Notification from A to Z

David Behinfar, JD, LLM, CHC, CIPP  
University of Florida  
College of Medicine – Jacksonville  
UF Privacy Manager  
(904) 244-6229  
david.behinfar@jax.ufl.edu

# Presentation Summary

- High-level Summary of the federal Breach Notification Rule
- Procedural History & current Status of the Breach Notification Rule
- Is this the end of the Harm Threshold ? ? ?
- Why the Harm Threshold fails to protect all patients
- How California is the real trailblazer when it comes to notifying patients of medical privacy breaches and why HHS may soon join CA on this trail.
- Once you get to the actual point of notifying patients . . . what are some practical points of a breach response and notification that you may want to consider sooner (like before a breach occurs) rather than later.

## What's not covered in this presentation? State Breach Notification Laws . . . Except for a passing reference to CA breach notification laws

- Notification/Reporting requirements for a breach of patient information are set forth in a number of state statutes across the country.
- Some state breach notification laws are directed at consumer data, others are directed at electronic consumer data, and some are focused on medical data and many of the laws are some combination of this group.

# HITECH Breach Notification Summary

Upon “discovery” of a “breach” of “unsecured” PHI – the CE must issue notification to affected persons (and HHS and possibly the media)

- What is a Breach?
  - Unauthorized acquisition, access, use, disclosure of PHI;
  - In a manner not permitted by the HIPAA Privacy Rule;
  - That compromises the security or privacy of such PHI (which HHS has interpreted as a harm threshold).
- Encrypted or Properly Disposed / Destroyed data is Secure.
  - Exceptions:
    - Unauthorized person would not reasonably have been able to retain the PHI (ex. EOB sent to wrong person – returned to CE in unopened envelope)
    - Certain good faith or inadvertent access by or disclosures to workforce in same covered entity/business associate and is not considered an inappropriate use or disclosure

# HARM THRESHOLD

- CE must assess whether the Harm Threshold has been met: The Breach must pose a significant risk of harm (financial, reputational, or other harm) to the individual.
- Fact-specific risk assessment must be undertaken (where the CE considers type & amount of PHI, recipient of PHI, and any mitigating circumstances).

# Notification

- Notification to affected individuals
  - Written notice (primary method)
    - Electronic notice if agreed to by the individuals
    - As soon as reasonably possible – not later than 60 days
  - Notification to the media - if more than 500 residents in a State or jurisdiction
  - Notification to HHS required
    - for breach > 500 must notify HHS IMMEDIATELY (contemporaneously with notice to individual)
    - Will be posted on HHS wall of Shame:  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>
    - If < 500 - submit to HHS in Log annually (by March 1 following the calendar yr)

# Notification cont . . .

- Substitute notice
- Law enforcement delay
- Content requirements for the notice:
  - Description of what happened
  - Type(s) of PHI involved
  - Steps individual should take to protect themselves from harm
  - Description of investigation by CE
  - Contact procedures for people to ask questions

## Procedural History:

### Breach Notification for Unsecured Protected Health Information; Interim Final Rule


- The Interim Final Rule for Breach Notification for Unsecured Protected Health Information was issued pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act.
- Interim Final Rule - Issued August 24, 2009.
- Effective 30 days after publication on September 23, 2009.
- Public comments were accepted for 60 days following publication until October 23, 2009.
- HHS delayed enforcement (akin to prosecutorial discretion) and stated that they would not impose sanctions for failure to provide the required notifications for breaches discovered through February 22, 2010.
- HHS still expected CEs to comply with the rule beginning on September 23, 2009 – it was just that HHS was not going to begin imposing sanctions until February 22, 2010.

## Procedural History continued . . .

- During the 60-day public comment period on the Interim Final Rule, HHS received approximately 120 comments.
- HHS reviewed the public comment on the interim rule and developed a final rule, which was submitted to the Office of Management and Budget (OMB) for regulatory review on May 14, 2010.
- On July 28, 2010, HHS announced: At this time, HHS is withdrawing the breach notification final rule from OMB review to allow for further consideration.
- Until such time as a new final rule is issued, the Interim Final Rule that became effective on September 23, 2009, remains in effect.

# Why did HHS pull the final draft version of the rule at the last minute? Here's what I think happened . . . Sebelius reconsidered . . .

- A striking criticism of the Rule came in a letter dated October 1, 2009 signed by several members of the House of Representatives, including: Henry Waxman (D-Calif.), Joe Barton (R-Texas), Charles Rangel (D-N.Y.), Pete Stark (D-Calif.) John Dingell (D-Mich.) and Frank Pallone Jr. (D-N.J.)
- Copy of letter:  
<http://www.modernhealthcare.com/assets/pdf/CH674761030.PDF>
- The Congressmen indicated that when drafting this legislation they considered a “harm threshold” and rejected it. They then urged Sebelius to repeal the harm threshold “at the soonest appropriate opportunity.”
- HHS Secretary Kathleen Sebelius thanked the Congressmen in a written response dated October 20, 2009 and indicated that their letter would be added to the public comments.  
<http://www.modernhealthcare.com/assets/pdf/CH674751030.PDF>



So we clearly have several  
members of Congress who  
steadfastly oppose the Harm  
Threshold . . .

# Are there any other problems with the Harm Threshold?

Consider this example:

A physician at your San Francisco based hospital loses an unencrypted laptop with a database containing patient names, their home address and the past three years of whether the patients have received a flu shot - with 5,000 patients in the database

Here's what it might look like for a single patient :

Name:	Address	Flu Shot data from SF Primary Care clinic
1. David Wolfe	111 First Street, San Fran, CA. 80001	2010 - yes with H1N1 (August 1, 2010) 2009 - yes (July 31, 2009) 2008 - yes (August 21, 2008)

# Let's run through the “harm threshold” analysis for this example

- We can assume that this is a breach, right?
- Now we have to determine whether the breach compromises the privacy or security of the PHI . . . So, let's figure out if there is a significant risk of:
  - Financial Harm: (no social security, bank account or credit card information).
  - Reputational Harm: (would a patient really care if someone finds out that he or she got a flu shot?)
  - Other Harm: (can't think of anything).


# But, can we be sure of these conclusions in our risk assessment ?

- Should we look into the charts of any patients to see if maybe they have something in there to suggest that there could be potential damage to their reputation?
- Should we call friends & neighbors of the patients and poll them to see if whether they found out such a thing about the patient whom they know – whether it damage that patient's reputation?
- This begs the questions of whether the application of the Harm Threshold is meant to be objective or subjective.
- If it is subjective – then perhaps we should consider each patient's individual circumstances
- If it is objective, then the CE can make some broad based assumptions and presume whether there is a “significant” risk of harm – without really considering anyone's individual circumstances.

# What does HHS say in the commentary to the rule . . . Objective or Subjective . . . ?

- HHS says: “The risk assessment should be fact specific, and the covered entity or business associate should keep in mind that many forms of health information, not just information about sexually transmitted diseases or mental health should be considered sensitive for purposes of the risk of reputational harm . . . 74 FR 42745
- There’s also a reference to OMB Memorandum M-07-16 for factors to consider whether a significant risk of harm is present  
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/mo7-16.pdf>

Neither of the above really tell us very much about whether the application of the Harm Threshold should be objective or subjective. . .



But aren't you sitting there and saying – it really doesn't matter in this example because whether someone got a flu shot is so trivial that it could never result in reputational, financial or other harm to an individual.

Seriously who could possibly care about flu shots?

# Now Consider who David Wolfe really is . . .

Is it possible to stop getting sick? What would it be like to accomplish life free of physical setbacks and full of productive energy?

**There is someone who has not been sick at all for the last 15 years . . .**

Who is he? His name is **David Wolfe**, and if you don't know him, he happens to be the most recognized super-nutrition authority whose fans and clients include T. Harv Eker, Tony Robbins, Angela Bassett, Woody Harrelson, and hundreds of thousands more.

He reveals step-by-step what to eat and what to do for immediate immunity transformation.


David Wolfe has been a professional nutritionist for over 16 years now and is a highly respected raw food and superfood guru (or as he calls it, a “gastronaut”). Known as David “Avocado” Wolfe or “The Chocolate Man,” his knowledge is extensive and he believes powerfully in the statement, “**what you eat becomes you.**”

He said, “**I’m never sick. Ever. I’ve pre-loaded my body with superfoods and superherbs.**”

<http://myliferecipe.com/david-wolfe-superfoods/>

Now, Do you think that Mr. Wolfe will possibly suffer any of the following:

- Financial harm – yes
- Reputational Harm – yes
- Other Harm – probably
- Knowing what you now know – would you notify Mr. Wolfe of the lost laptop containing his information on the flu shots he has received?



So, not only do we have Congressmen who oppose the Harm Threshold . . . but if you buy into my example . . . we also have a Harm Threshold that doesn't really work to protect all patients because it is only designed to address probable harm not actual harm.

# Now consider these two approaches to breach notification:

Approach # 1. The CE decides whether to notify patients based on an “objective” analysis of what the potential risk of harm may be and then makes decision on whether to notify.

Approach # 2. There is no harm threshold and all patients are notified of every breach – so they can make their own decision on what the level of risk is to them.

# Is it even possible for a CE to notify patients of each and every breach?

- From January 1, 2009, when law SB 541 went into effect, through May 31, 2010, health care facilities have reported a total of 3,766 breaches. The law (with companion bill AB 211) calls for health care facilities to prevent unlawful access, use, or disclosure of patients' medical information and to report violations to CDPH and the individuals affected w/in 5 days after the breach has been detected.
- The California Department of Public Health (CDPH), which enforces the law, receives notification of about seven breaches a day.

<http://www.healthleadersmedia.com/content/TEC-255666/With-No-Harm-Threshold-Nearly-All-Breaches-Substantiated-in-CA>




If California can do it . . . Why can't  
the US federal government?


We may soon have that answer.

If you think the Harm Threshold will remain in place. . .  
you may want to consider taking a look at these web  
sites with sample “Risk Assessment Tools”

- NCHICA Risk Assessment Tool:  
[http://www.nchica.org/HIPAAResources/Documents.  
htm](http://www.nchica.org/HIPAAResources/Documents.htm)
- University of Louisville Breach Notification Tool:  
[http://privacy.louisville.edu/Resources/UofL%20Breach  
%20Notification%20Tool.pdf](http://privacy.louisville.edu/Resources/UofL%20Breach%20Notification%20Tool.pdf)



Let me now try and give you  
some practical advice on breach  
notification.



Let's say one way or the other you now have to notify patients about a breach – what are some important elements of your breach notification process that you should consider (that you won't find in the rule)?

1. Computer Forensics. Have a plan in place to address the need for Computer Forensics. If you lose possession of an unencrypted laptop & you later regain possession of the laptop – how do you know whether or not someone accessed the PII or PHI on the laptop? If you can get computer forensics results BEFORE you send out your letters – that would be ideal because you may not need to send the letters at all. Your IT personnel may know of reputable computer forensics labs or persons who can perform this service for your institution. So make sure you know who you will call for a forensics examination BEFORE a breach occurs.

2. Contracting with a Call Center. If you think you can internally handle calls on a breach involving 100,000 patients – more power to you. If not, you'll need to think about contracting with a call center. Things you can consider with your contract: performance bond, call center in US (sorry - nothing against India), privacy breach experience, has more than 1 physical call center, references, able to answer calls 24/7 including holidays, multilingual staff, project manager, escalation process, will provide customized reporting for you, provides detailed pricing for all team members, will train call center employees on your specific breach, will assist with script writing. Call center services can get expensive – so my recommendation is that you send out an RFP and know who you will use BEFORE you hit the jackpot on a privacy breach at your facility.

3. Printing & Mailing the Breach Notice. If you need to print out 100,000 letters this is not an easy task. Will you personalize each letter or just have a “Dear Patient” introduction? Who will put together the list of patients and do the mail merge? You need to determine whether your organization will handle the mailing itself – or whether it will be contracted out in whole or part. Ask your mailing center what their capabilities are and their advance notice requirements. (Good Luck sending breach notices when patient statements are going out). Also use quality bond paper – otherwise the letter may look like a phony letter.

4. Press Release. Make sure you quickly involve your PR Dept so you can coordinate the timing of mailing the breach notice with the issuing of the press release. If you don't have a PR dept – then you need to consider how you might proceed with any media relations.

5. Police Report. If you fill out a police report – you could be tipping your hand to the media. So be prepared – this may force your hand on the press release. You need to understand this before you complete the police report.

6. Identity Theft Insurance or Credit Monitoring. Will you offer recipients of the breach notice this option? If so, you should have a vendor(s) lined up in advance. The letters you send out will have to give them instructions on what to do if they want this protection. There are several vendors in the market – and there is a difference between vendors. Also – consider implications of offering this to your patients – will you have to do it every time? Who will make this decision ?

This may be academic – as it may be built into the new federal breach reporting laws:

see the Data Security and Breach Notification Act of 2010

[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111\\_cong\\_bills&docid=f:s3742is.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s3742is.txt.pdf)

# Lastly, think about the value of credit monitoring insurance

- 3/9/2010 LifeLock, Inc. has agreed to pay \$11 million to the Federal Trade Commission and \$1 million to a group of 35 state attorneys general to settle charges that the company used false claims to promote its identity theft protection services.
- “While LifeLock promised consumers complete protection against all types of identity theft, in truth, the protection it actually provided left enough holes that you could drive a truck through it,” said FTC Chairman Jon Leibowitz.
- Are you simply paying for someone to place fraud alerts on accounts – which any individual should be able to do themselves

<http://www.ftc.gov/opa/2010/03/lifelock.shtm>



So we've covered a lot of information . . .

Anyone have any questions . . .