David Behinfar, JD, LLM, CHC, CIPP

University of Florida College of Medicine – Jacksonville

HIPAA Compliance Manager

(904) 244-6229

david.behinfar@jax.ufl.edu

Institution & Recent Patient Notifications of Privacy Breaches

- Univ of FL COM – Jacksonville
  - Academic medical ctr.
  - UF COM campuses in G'ville & Jax
  - 700 faculty, residents allied health professionals
  - 1,200 clinical & billing support staff
  - Research
  - Affiliated w/ Shands Healthcare 696 bed - level I trauma ctr.
  - 35+ on-campus & satellite clinics throughout Jacksonville

- UF JAX Recent Patient Breach Notifications in the News
  - (May 20008) Computer w/ unencrypted photos on 2000 plastic surgery pts donated to local family by physician
  - (June 2007) Computer Hard drive stolen 1000 pts

- UF G'ville Recent Patient Breach Notifications in the News
  - (June 2008) PII of 12,000 students available on-line

So, how is a Breach Response Involving 50 patients different from one involving 2,000, 20,000 or 200,000 ?

Planning Ahead is the Key

It is like the difference between cooking dinner for 5 people and 5,000 people

- You can easily address minor problems on the fly if you are serving dinner to 5 people – and you don't need to fully plan out every detail of the dinner.
- But when you cook for 5,000 people, issues arise that were not an issue when you cooked for 5 people – you have to plan all aspects of the dinner from start to finish. The same principle applies when you jump from a privacy violation involving a few hundred patients to one involving thousands of patients.
- When you cook for 50,000, or 500,000 or even more people it is a whole different ballgame altogether.

So PLAN AHEAD !

What do you need to consider when planning ahead PRIOR to experiencing a privacy breach involving 1,000's of patients ?

1. Breach Notification Laws. Understand what your st. breach notification statute requires – strict timelines (FL law requires notification w/in 45 days; substitute notice allowed when 500,000 or more pts involved or cost is more than $250,000.) Of course Fed Law may pre-empt the st statutes - stay tuned. Your policy on Breach Investigation/Response should mirror these timelines. By the time the breach makes its way to your office a few days may have passed – maybe even a week or more. Patients can become upset at why they were not notified sooner (a few weeks can make a difference for someone who receives a breach notice). Media seems to pick up on this frequently.

2. Computer Forensics. If you lose control of a laptop that is not encrypted & 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. You will need a written report also – again – the clock is ticking . . . This could easily eat up a week or more - so make sure you know who to call for a forensics exam BEFORE a breach occurs.

3. Patient calls. If you cannot find enough people in your organization to field phone calls – or at least act as a messaging service that can take names for you to call back – then you might need to contract for this service with a call center. This is not a good option, and should be used as a last resort. At a minimum, you need to think about where you could recruit people in your organization to field calls for a few days. Not to mention considering the capabilities of your hotline #. You might need the capability to have 5 – 7 lines available after a breach for a few weeks. One Alternative is to use a web site as your primary source of disseminating information and the call center as secondary source (See Univ of Miami website lost backup tapes www.dataincident.miami.edu).

4. Printing & Mailing the Breach Notice. If you need to print out 100,000 letters this is not an easy task. Will you personalize each ltr – or just have a "Dear Patient" introduction? Who will put together the list of patients? Will you include an informational brochure on identity theft or other material educating the recipient on identity theft? 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). If you use a vendor – will they sign a BAA ? This can take time . . . All while the 45-day breach notice clock is running . . . .

5. 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 to proceed with any media relations – good luck !
6. 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.

7. 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. Some offer credit monitoring (reactionary)– others offer identity theft protection (i.e. - before credit is offered to identity thief – phone call goes to Vendor – who contacts intended victim to ask if it is OK for bank or other entity to offer credit – don't open acct unless you have my permission). Also – consider implications of offering this to your patients – will you have to do it every time? Who makes this decision ?

8. Web Page – Posting Information bout the breach & FAQs. How about your website – are you going to place the notice & FAQs on your privacy website or your institution's website? If so – you will want to direct people who receive the notice & the media in your press release to the website – so this decision needs to be made early on so you can direct people to the right website in your notice.

So, what are some of the differences in how you might respond to a privacy breach involving 1,000's of patients vs a smaller number of patients in the 100's?

50 patient breach

- Investigation – probably no real difference BUT – make sure you have contacts with computer forensic personnel
- Written Notice – no problems here
- Taking calls from people who receive letters – no problem you can handle it
- Credit Monitoring / identity theft insurance – for 50 people the cost is negligible
- Press Release & Media Plan can be much more flexible

5,000 or 50,000 patient breach

- Investigation - Computer forensic investigation might help you avoid notifying patients if you can prove no access to electronic information
- Written Notice becomes much more difficult. Everything from compiling patient names/addresses to mailing letters – do you have a reliable vendor in place?
- You cannot handle calls in a breach involving 50,000 patients – but you probably could handle 5,000 pt breach – with some help – but you definitely need a toll-free hotline # & a few days of free time to answer calls – more than that – you might need outside help.
- Credit monitoring /identity theft insurance can be expensive for 1,000's of people
- Press release & handling media will become a priority very early on

Final Thoughts

Go though a fire-drill for a privacy breach at your institution that involves a breach of 50,000 patients. Can you honestly say that if a breach involving 50,000 patients occurred at your institution that you know who would:

- perform a computer forensics exam;
- handle all aspects of the mailing (printing the letters & envelopes, stuffing the envelopes – paying for postage);
- take patient calls or which outside vendor you might use;
- whether identity theft insurance would be offered & who that vendor might be; or
- who would make a press stmt & what media outlets would it go to? ? ?

- - - If not - then you really should start thinking about it . . . NOW