# The Fifteenth National HIPAA Summit

## Healthcare Security Professional Advanced Problem Solving Roundtable

**December 12, 2007**

# Roundtable Members

- **Walt Padworski –** Information Security Officer, Frankford Hospital, Langhorne, PA
- **Jim Reiner –** Information Security Officer, Sacramento County, Sacramento, CA
- **Jud DeLoss, Esq. –** Attorney/Principal, Gray Plant Mooty, Minneapolis, MN
- **Chris Apgar –** President, Apgar & Associates, LLC, Portland, OR
- **Marc Goldstone, Esq. –** VP and Assoc. General Counsel, Community Health Systems, Franklin, TN
- **John Parmigiani –** President, John C. Parmigiani & Associates, Ellicott City, MD (moderator)

# Approach

- We have created a starter set of “problems” for discussion
- We encourage your interactions/perspectives with the discussion to further examine and develop solutions to the above problems
- The hope is that additional “problem” areas will be identified that either stem from the above discussions or are new

# Problem #1

Your corporate counsel calls and tells you that the hospital is being sued. She tells you that she just left a discovery meeting and the opposing attorney has asked her to produce a log showing who accessed a particular patients electronic medical record while he was in the hospital and also wants copies of any email, voice mail, or text message that even mentions the patient. She tells you to preserve all of the electronic correspondence created by anyone involved until told otherwise. The catch? The patient in question is a movie star who was treated by your hospital a couple of weeks ago.

What do you do?

# Problem #2

You are the CIO of non-profit hospital. In most, if not all of the audits I.T. has undergone over the last several years, the need to better manage access controls was mentioned or alluded to in audit observations.

Now you've just received a report conducted by an external auditor that was looking at your departments General Controls surrounding the maintenance of a financial application. The audit cites four specific observations and labeled each as a " SAS112 control deficiency " - The observations dealt with mismanaging user access to I.T. Systems, inconsistent log review, failure to produce support documentation, and failure to perform periodic penetration testing.

What steps do you take?

# Problem #3

Your annual audit of user access to your medical records system indicates users from non-HIPAA components of your company are not only accessing the ePHI (which they have no business doing), but they also have changed some patient bills.

What do you do to get control of this?

P.S. This is a real problem whenever a government organization is a hybrid entity instead of the entire organization being covered by HIPAA.

# Problem #4

The hospital administrator has had difficulty getting physician/surgeon "buy in" with the hospital's new EHR system. One surgeon has been particularly problematic. She refuses to directly access the EHR and relies upon a variety of nursing staff (both her own and the hospital's) to access the EHR. In order to do so, the surgeon has given several nurses her ID and password. Recently, the surgeon has been reading up on the Security Rule and now claims that she needs immediate, emergency access to the EHR just prior to her surgeries due to their delicate nature and the need for medical information to successfully conclude the surgery. She claims that she is entitled to "break the glass" in these situations and bypass any security measures in place because they are so "problematic" she could not access the information otherwise.

How would you advise the hospital administrator to address these issues with the surgeon and the staff?

# Problem #5

Steve Gates (a distant relative of Bill Gates, or so he claims), is the assistant shipping and receiving clerk on the midnight shift at Medical School of Daughters of Samaritan Medical Center (MS-DOS MC). One night, at about 2:00 a.m., a message pops up on this workstation advising him that his computer contains evidence of every salacious website he's ever visited, and asking him to "click here" to install the latest Windows Update to eliminate such offending material. He does, and then, in an effort to earn a promotion to deputy shipping and receiving clerk, he heads over to each of the patient care units, sits at the unit secretary's desk, and carefully enters the website address that was in the popup box, to install this important "safety patch" on each machine in the 4 acute-care floors of the hospital. What to do next with this “patch management” problem?

# Problem #6

You are conducting a site audit at one of the high risk clinics in a needy part of town. You find the door to the network closet is not locked - standing open in fact. Then you see a wireless router has been installed right next to your own WAN router. An AT&T line has been installed as well. You find out that a separate organization comes into your clinic on the weekends to provide free health services to the community. They use your facility unsupervised. Politically this will continue. No way to stop it.

So, how do you get control of access to your network closet, placement of the first of many 'rogue' wireless routers, access to your patient folders, and access to your pharmacy?

# Problem # 7

Your institution has just been informed that the OIG will be coming in two weeks to conduct a HIPAA security audit.

As the CSO, what should you do to get prepared; who should you get involved; and what areas should you be focusing on with so short a lead time?

# Thank You!

**Walt Padworski** wpadworski@fhcs.org 215-949-5194
**Jim Reiner** reinerj@saccounty.net 916-874-7752
**Jud DeLoss** jud.deloss@gpmlaw.com 612-632-3389
**Chris Apgar** capgar@easystreet.com 503-977-9432
**Marc Goldstone** marc_goldstone@chs.net 615-465-7352
**John Parmigiani** jcparmigiani@comcast.net 410-750-2497