

# Documenting HIPAA Readiness

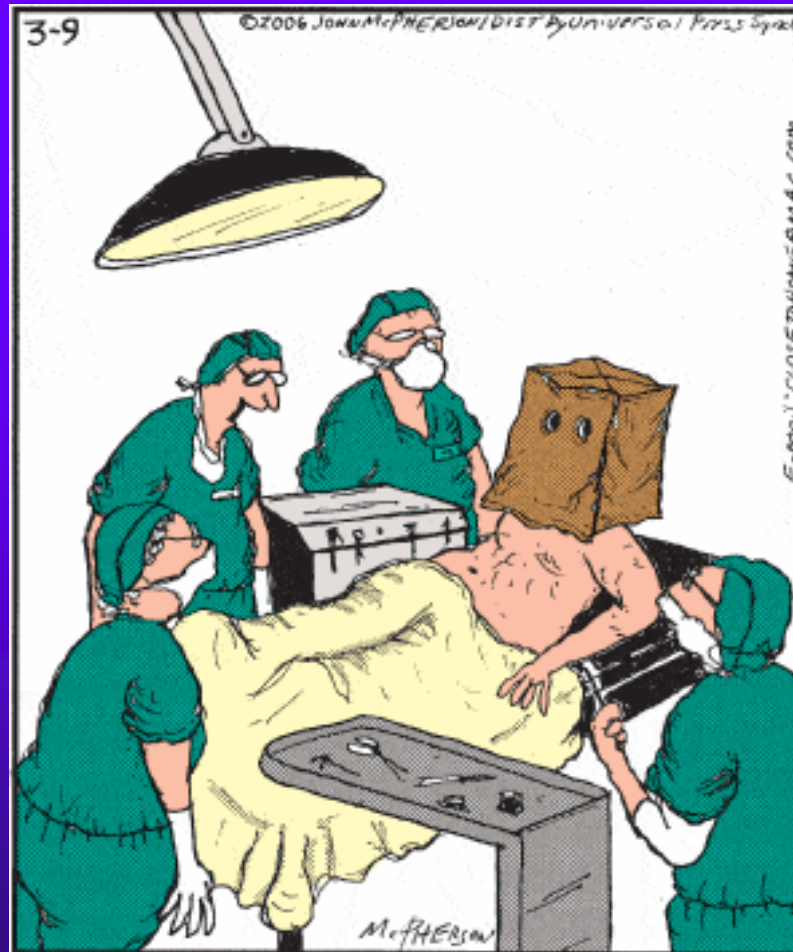


## What to Tell Your Business Partners

*Philip J. Nesser II, CISSP*

Information Security Officer  
Group Health Cooperative

# The (*not quite*) Reality



"I realize it's a bit strange, sir, but due to the new health information privacy laws, none of us is allowed to know your identity."




# The Theme

- ◆ How do you disclose enough information to your business associates and partners
  - to make them comfortable with your HIPAA readiness;
  - without providing too much proprietary information?



# The Fundamental Problem Business Partners

- ◆ What they really want is an assurance that their information is private and secure
  - Shows a basic lack of knowledge of what HIPAA really covers
- ◆ We can't do that!
  - No security is 100%
- ◆ The best we can do is tell them we are HIPAA compliant, or ready



# The Fundamental Problems HIPAA Readiness

- ◆ There are no federally mandated reporting requirements
- ◆ There are no state mandated reporting requirements
- ◆ There are no industry standard reporting requirements

*So everyone is making it up as they go*



# The Worries (1)

## 45 CFR Parts 160, 162, & 164 III. A. 3.

- ◆ In meeting standards that contain addressable implementation specifications, a covered entity will ultimately do one of the following:
  - (a) Implement one or more of the addressable implementation specifications;
  - (b) implement one or more alternative security measures;
  - (c) implement a combination of both; or
  - *(d) not implement either an addressable implementation specification or an alternative security measure.*



# 45 CFR Parts 160, 162, & 164

## III. A. 3.

- ◆ In all cases, the covered entity must meet the standards, as explained below.
  - *The entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework.*
  - *This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation.*



## The Worries (2)

- ◆ Public disclosure
- ◆ Legal ramifications
  - Particularly in actual litigation
- ◆ Competitive advantage (or disadvantage)
- ◆ Loss of staff time and energy
- ◆ Answers can lead to more questions
  - Almost an invitation to do so



# The Question: *What to disclose?*

## ◆ NOTHING!

- Or less!
- *If possible*

## ◆ Why?

- There is no upside to any disclosure that isn't necessary for meeting fundamental business and contractual obligations



# The Path To The Answer

## *What you need to know*

- ◆ Information about the requestor
  - Who they are
  - What is the business relationship
    - Customer, vendor, partner, patient, government, press, etc...
  - Why do they want to know
    - Their own auditing? Risk assessment on their part? Public disclosure? Personal concerns? etc...



# The Answers: *(Sometimes)*

- ◆ SAS 70 (Type I or Type II)
  - Statement on Auditing Standards (SAS) No. 70, *Service Organizations*
    - Expensive (\$75,000+)
    - Very time consuming (Especially Type II)
    - Will satisfy most requestors
    - Covers a much wider set of topics than is typically needed



# The Answers: *(Sometimes)*

- ◆ Internal Audit Report Summary
  - Only provide executive summary section
- ◆ External Audit Report Summary
  - Same technique as with Internal Audit
  - Carefully selected pieces (i.e. remove all financial information)



# The Answers: *(Sometimes)*

- ◆ Boilerplate letter from CIO and/or CISO
  - With support from your legal team
  - Outline general steps taken to achieve HIPAA compliance
  - Outline other standards your organization complies with
  - Outline your auditing strategy
  - Summary of outside legally required audits (i.e. OIC)



Questions?  
Discussion?

*Any other answers?*