The “Reverse Loophole” - HIPAA Security Risk and Regulation Awareness of Interconnected Healthcare Environments

G. M. Ludlow[1], R.C. Skinner[2], D. Hadaway[3]

[1] CERIAS InfoSec M.A., School of Philosophy, Purdue University, West Lafayette, IN 47907
[2] CERIAS InfoSec M.S., Department of Computer Technology, School of Technology, Purdue University, West Lafayette, IN 47907
[3] President, infotex Inc., infotex.com, 1250 South Creasy Lane - Lafayette, Indiana 47905

Problem

This project investigates the relationship between large and small healthcare providers in relation to the HIPAA security ruling. Contained within the ruling is a provision that, to be HIPAA compliant, a healthcare provider must ensure that all parties the organization does business with are also compliant. The deadline for compliance for large providers is April 2005, and the deadline for small clinics is April 2006. These two factors create a “reverse loophole” effect. For the large entities to comply and continue their current business practices, they must in some way convince small clinics they do business with to become HIPAA compliant a year earlier than they are otherwise obligated. Our project explores the dynamics of this relationship in order to develop the means for large healthcare providers to address this potential problem.

When the security ruling was finalized, additional requirements were put on healthcare providers. Without a plan or method of addressing non-compliant business partners, large healthcare organizations are at risk for at least the one-year window. One of the goals of this project is to find a way to reduce or eliminate that risk.

HIPAA Security Principles

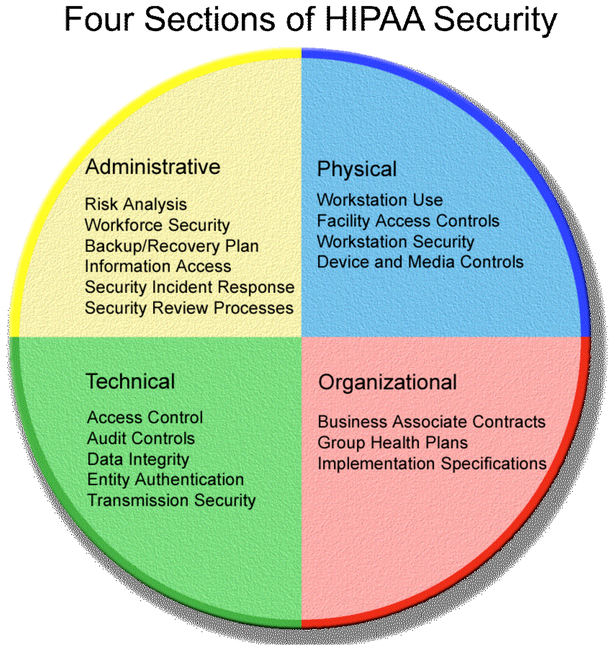

Figure 2 – HIPAA Security Principles

The Healthcare Insurance Portability and Accountability Act of 1996 mandates significant changes that govern the provision of health benefits, the delivery and payment of healthcare services, and the security and confidentiality of individually identifiable, protected health information. Privacy compliance deadlines have recently passed and now it is time to concentrate on security.

HIPAA Security Compliance Deadlines
- February 20, 2003 - Department of Health and Human Services (DHHS) issued the Final Security Rule
- April 21, 2005 - Security Standards - all covered entities except small health plans
- April 21, 2006 - Security Standards – small health plans

Compliance Environments Scenarios

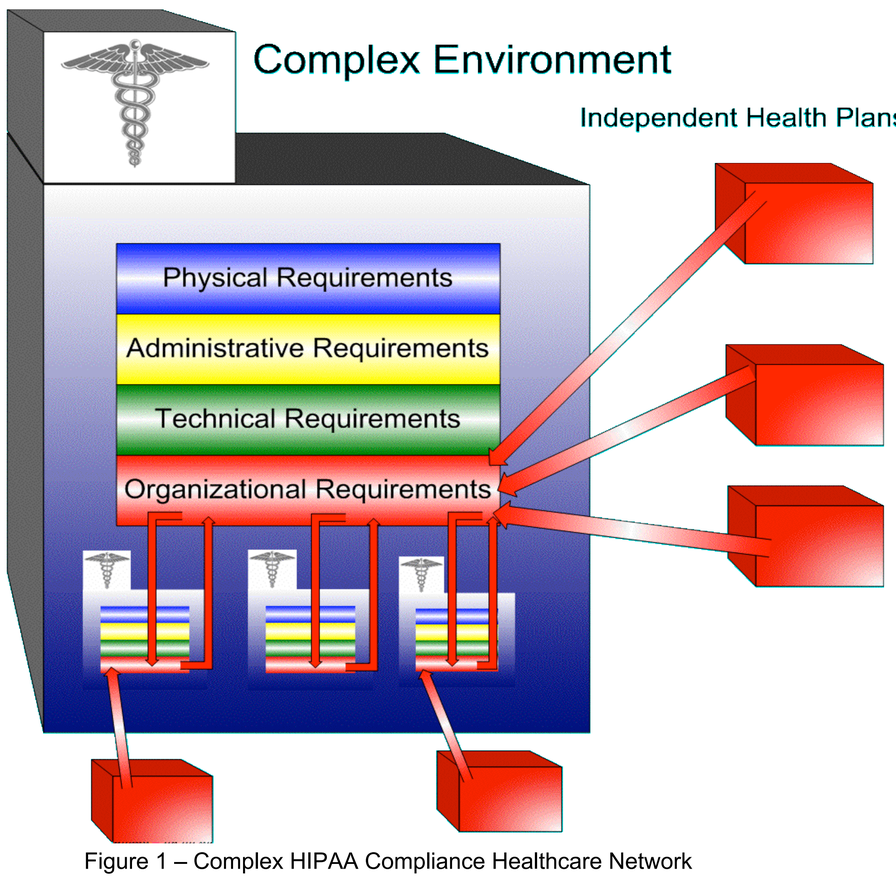

Figure 1 – Complex HIPAA Compliance Healthcare Network

In a healthcare group comprised of several smaller clinics (Figure 1), each individual clinic and all the health plans they share information with must meet certain security standards. If any one of the red-colored portions in the figure are non-compliant, the entire healthcare provider and all smaller units will not meet HIPAA requirements.

Project Plan / Scope

This project is a cooperative effort between CERIAS students and **infotex** (a CERIAS sponsor). Dan Hadaway of infotex will help direct and consult with Rich Skinner and Gram Ludlow throughout the project.

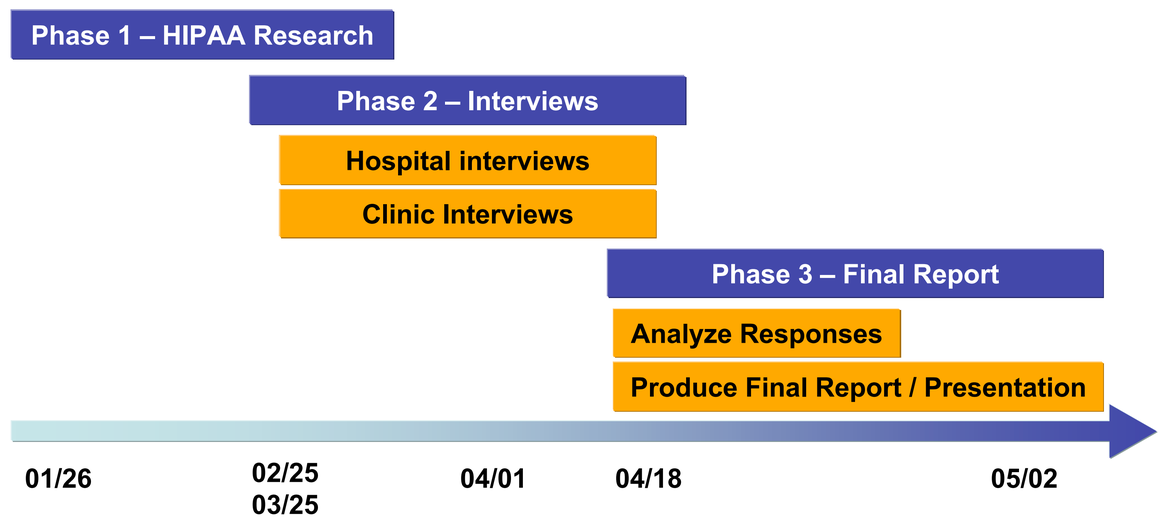

Figure 3 – HIPAA Security Project Plan

The project has three main phases (Figure 3): Preliminary HIPAA research, data gathering through interviews, and creating a final report. HIPAA research will be done with primary and secondary HIPAA Security texts, both from industry and academia. For the interviews, representatives from two hospitals and several small clinics will meet with the project team to discuss their unique needs. The research team will interview officials from two hospitals and several small clinics, including CIO’s, IT managers, compliance officers, doctors, practice managers, and end users. Any data not learned directly through interviews will be gathered through follow-up questionnaires and surveys. In the final part of the project, the needs of both the large and small health plans will be balanced and a report will be produced. In addition to this report, recommendations will be made to the hospitals for the best way to proceed with the organizational requirements of HIPAA.

PURDUE UNIVERSITY

CERIAS

infotex

Discovery Park e-Enterprise Center