# The Health First Case Study: Teaching HIPAA Regulation with Security Planning

S. J. Lincke, *University of Wisconsin-Parkside*

***Abstract – HIPAA is an example of full-featured security regulation that is also concerned with privacy. Exposing students to this real-world regulation helps students to realize that the security that they are learning is actually required by law. It also provides them useful knowledge for when they interview, and enter the workforce. The Health First Case Study enables students to work with a hypothetical Doctor's office, which must adhere to HIPAA. Through the case study exercises, students continually refer to the HIPAA regulation, to ensure that they are in compliance. The case study also helps students to understand the perspective of the business owner, and plan for security with the aid of the Small Business Security Workbook.***

**Index terms – HIPAA, case study, security planning, audit, security education.**

## I. Introduction

The Health Insurance Portability and Accountability Act (HIPAA) is important privacy and security regulation for health in the U.S. The CSI Computer Crime and Security Survey reports that 57.1% of respondents must comply with HIPAA (although only 7.7% of respondents categorized themselves as a 'health service' industry) [1]. HIPAA has additional advantages for teaching in that it is full-featured and values privacy. This NSF-funded project has developed a hypothetical case study, based on a doctor's office, to help students understand the HIPAA regulation. This paper reviews parts of the Health First Case Study that focuses on HIPAA.

Case studies have been used in business since the 1930s [2,3], and in engineering [4]. Lu and Wang [2] point out that case studies enable student-centered learning, by promoting interactivity between students and faculty, reinforcing educational concepts taught by lecture, and deepening student understanding by building knowledge into students. Students not only learn to apply theoretical knowledge to practical problems, but also to be creative in discovering solutions. Wei et al. [3] agree that case studies "constitute the basis for class discussion." They add that cases help students transition to the workplace, by exposing students to diverse situations, thereby enhancing adaptation skills to new environments, and increasing students' self confidence in dealing with the world. Students increase their communications skills, which includes listening and persuasion skills. Chinowsky and Robinson [4] stress that case studies enable interdisciplinary experience, which students are more likely to encounter in the real world. In the civil engineering real world, engineers must cope with regulation, architects, schedule and financial constraints, and the owner. They stress the importance of using real-world artifacts in the case study.

We are aware of four sets of case studies relating to security. Dhillon [5] has written a security text that describes a company's basic scenario as an introduction to each chapter. At the end of each chapter is a case study problem, which has students consider specific aspects related to the case study. ISACA also provides graduate-level teaching cases [6,7], which emphasize corporate governance problems related to security management and COBIT. However, understanding law, in addition to security technology, is also important for IS security students [8,9]. Schembari has students debate legal case studies, to help them learn about security-related law [9]. The goal of the Health First Case Study [10] is for undergraduate CS/IS/IT students to plan security for a HIPAA-adhering doctor's office, with the help of the Small Business Security Workbook [11]. This Workbook has been tested with real small businesses, via service learning, in addition to the case study [12].

The Health First Case Study strives to accomplish many of the goals described for case studies. Students do learn to apply concepts to the real world, following a lecture. Using active learning, students work in groups and use the case study and Small Business Security Workbook to discover new solutions that often vary by group. The Workbook leads students through a design, and the case study provides the context.

The case study achieves the interdisciplinary aspect, by enabling students to experience multiple perspectives: the doctors', HIPAA regulation, IT and financial, including through the use of real artifacts: business documents. In this case study, students plan security for a doctor's office, which must adhere to HIPAA. HIPAA is important because approximately 58% of organizations must adhere to it, and it is representative of regulation that

*University of Wisconsin-Parkside, 900 Wood Rd., Kenosha WI 53141.*

is concerned with state-of-the-art privacy and security. Through this law, students understand that security procedures are important, including risk, business continuity, physical security, and personnel security. Very often students consider security as focusing solely on technology: network security and security tools. HIPAA broadens this outlook.

Students also experience the perspective of the business owner. The case study is provided as conversations between a doctor, a registered dietician, a medical administrator, and an IT specialist. Students learn that a solution is not just about technology – it is also about the business. Business and technology costs are provided for students to work with, including business financial reports.

The case study helps students to transition to the real world; we measure success in the service learning aspect. Through the case study, students work on a real-live, complex problem. We use it as practice for students to work with a real community partner, as part of a service learning assignment. We have found that students rely on the case study to prepare them for the community partner encounter.

The material is not only meant to make students competent with HIPAA, but also to prepare students for ISACA's Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) exams [13,14]. This material discusses high level security materials, to prepare students for security analyst or security management positions.

The Health First Case Study can be used for a semester long introductory or intermediate course in security for upper-level undergraduates or graduate students. Alternatively, parts of the lecture materials and/or case study can be used in a course on Computer Networking, Network Security, and Software Engineering.

Health First is one case study in that it addresses one business: a doctor's office. However, it is a collection of case studies, since each case study develops some aspect of the security plan. The case studies can be used as active learning exercises or homework assignments, after each lecture.

With the Health First Case Study, students make important decisions regarding the security planning process. The case study uses two learning mechanisms: the Small Business Security Workbook, which leads students through the security planning or architecture process, and the Health First Requirements Document, where students enhance a requirements document to address security, for a specific software system. The case study is provided as conversations between the doctor and staff, and an IT person.

This paper includes a brief description of HIPAA, a description of the case studies most related to HIPAA, notes on teaching with the case study, our results, and a conclusion.

## II. Introduction to HIPAA

The HIPAA regulation was intended for insurance portability, but also includes security regulation. The HIPAA regulation has 5 sections, of which Title 2 "Preventing Health Care Fraud & Abuse, Administrative Simplification, Medical Liability Reform" relates to security. As background information, HIPAA Title 2 security is divided into two sections: Privacy Rule and Security Rule [15].

The Privacy Rule is concerned with individual health information privacy, whether or not computers are used. Thus, the Privacy Rule is concerned with access control and medical information usage (in paper or computer form) including standards for Patient Health Information (PHI) disclosure [15,16].

In contrast, the Security Rule addresses issues relating to electronic patient health information and computer systems. The Security Rule describes Administrative, Technical, and Physical Safeguards (or controls) related to computer use [17]. Each of these three safeguards is divided into Standards (e.g., Security Management Process, Security Awareness and Training, Facility Access Control, Transmission Security). Each Standard may be further subdivided into Implementation Specifications, which are specified as either Required or Addressable. Addressable options give more flexibility in implementation, but their implementation must be documented.

HIPAA is introduced in the beginning of our Information Security course as a 2-3 hour lecture. HIPAA provides an excellent overview of security, since it is concerned with both privacy and computer security. The HIPAA lecture is the first full lecture of the course to show the relevance and importance of each security topic taught during the course. It helps students to understand the importance of security procedures, in addition to security technologies. The HIPAA PowerPoint lecture is provided in exercises throughout the course so that students can refer to this regulation during case study exercises.

## III. Case Study Exercises

The HIPAA case studies address four areas: 1) strategic policy planning; 2) detailed security plans and procedure development; 3) software planning and design; and 4) audit. For each of the case studies described below, the students refer to the HIPAA lecture to complete each exercise, and thus the exercises continually reinforce

HIPAA concepts. The HIPAA case study exercises include:

*A. Strategic Policy Planning*

- **Analyzing Risk**: Risk is a requirement of the Security Rule's Security Management Process standard The HIPAA lecture reviews jail sentences and financial penalties for not being HIPAA-compliant. These probable costs factor heavily into the risk analysis process.

- **Security Program Development**: Editing a Policy Manual for HIPAA: Students modify a COBIT-based list of policies, to ensure adherence to HIPAA. Thus students tweak a summary of the COBIT policy, exposing them to both COBIT and HIPAA. The draft policy document already covers much of the Security Rule, but much of the Privacy Rule must be incorporated.

- **IT Governance**: Planning for Strategic, Tactical, and Operational Security: Students devise a plan to adhere to the regulation. Adhering to the full HIPAA Security Rule takes time. Thus, a phased approach is developed, so that the computer network and capability is expanded as more of the HIPAA Security Rule is implemented. For example, the doctor wants access to his medical database at the hospital, but cannot until most of the security rule is implemented. The Security Rule must be implemented in stages: no LAN, adding WLAN, adding outgoing access to Internet, adding incoming access into computer network.

*B. Detailed Security Plans and Procedures*

- **Designing Physical Security:** HIPAA **Physical** Safeguards are concerned with facility access control, workstations, and device and media controls. Students prepare a map with room sensitivity classifications and description of how physical safeguards are implemented.

- **Information Security, Network Security, Business Continuity, and Incident Response:** Other case studies involved with detailed security planning are provided as part of the Health First Case Study and Small Business Security Workbook. They address the Security Rule's Information Access Management, Device and Media Controls, Transmission Security, Contingency Plan standards. These, however, follow the Workbook and do not require review of the HIPAA lecture.

*C. Software Requirements and Design*

- **HIPAA: Updating Req. Doc. to adhere to Privacy Rule:** Students modify a Requirements Document to accommodate the HIPAA Privacy Rule. The main concerns are Discretionary Access Control: enable permissions to be set for access to specific data, and recording Disclosures.

- **Applications Control: Extending Req. Preparation by Planning for HIPAA Security Rule:** Students modify a Requirements Document to ensure that HIPAA Technical Safeguards (e.g., authentication, access control, transmission security, logs) and Administrative Safeguards (e.g., supervision controls, termination, information system activity review) are addressed. This is a longer assignment and can serve as homework.

*D. Security Audit*

- **Developing a Partial Audit Plan:** Students plan an internal audit to check adherence to an Implementation Specification of the Security Rule. As part of the **IT Governance: Planning for Strategic, Tactical, and Operational Security** case study described above, students plan a scheduled implementation of HIPAA, and select a set of Implementation Specifications to fulfill in the next 6 months. Students select one Implementation Specification for which to write an audit plan. An example audit plan for Physical Safeguards is provided in the Workbook appendix, as a reference for students.

It makes sense to do the case studies in the above order in the real world with experienced security staff. However, students find it easier to learn to work with focused details before working with higher level concepts. Therefore, we do two of the Strategic Policy Planning case studies at the end of the semester, with the more advanced PowerPoint lectures: Security Program Development and IT/Security Governance. The Risk case study can be done early in the semester.

Many computer science students intend to become programmers when they graduate. Thus, making the curriculum relevant to them requires showing them how security knowledge is useful to a programmer. Often they view many of these case studies as IT-related, and thus not important. The two exercises involving Requirements Documents shows them that knowledge of security can help them in designing secure software products. Thus, we incorporate a Requirements case study at the beginning of the course, and communicate through the lectures how security design is important for various topics.

## IV. Notes on Teaching the Case Study

We teach the case study as an active learning exercise in class, although it could be used as homework. The NSF-funded case study materials include PowerPoint lectures, case study, Small Business Security Workbook, and Small Business Requirements Document. There is also a Small Business Security Workbook Solution, which includes case study solutions.

A PowerPoint lecture is given in the first half of a 3-hour class, and the second half is the active learning exercise. The lectures have been enhanced to include appropriate example tables from the Small Business Security Workbook, for a University application. (The students will complete a Doctor's office application.) These examples help students to observe how tables are properly used, and may provide ideas for their solution (or not!) The lecture notes are made available to students from a web page during the active-learning exercise, and they are often referred to.

Students are grouped into 3-4 person teams, and each team is provided a computer to edit the Small Business Security Workbook directly on-line. All students should be able to see the display, so computers are selected and manipulated for the best display. The best computers tend to be the ones at the end of a row of tables, providing 3 sides for students to sit, discuss, and observe Workbook use.

The instructor provides a copy per student, of the 2-3 pages of the specific case study exercise. The beginning of each case study indicates the corresponding section in the Workbook to work with, but is also announced by the instructor. The case study has subsection headings to indicate the conversations for each subsection of the appropriate chapter in the Workbook. The Workbook is retained on the computer, so that students may add to the Workbook each week. This enables students to review previous decisions during case study exercises.

It is important that the HIPAA lecture is given before any of these case studies are given as an exercise. The HIPAA lecture notes are also made available to students weekly. We print up copies of the HIPAA lecture, with sufficient copies for one for each group. The HIPAA lecture copies are distributed at the beginning of each lab, and retained for reference in the teaching lab.

The best way to start the case study is to have students select specific roles to play. To encourage this, we have students read the first part of each case study out loud, where each role is read by a different student. Most case studies have 4 roles, so there would normally be 4 readers. This has the advantage that students get to play the role of the IT person, versus a doctor or medical administrator. It also starts out the case study with students actively talking, and not silently reading (or being confused). If the first part of the case study is read in front of the whole class, it enables the instructor the opportunity to start asking questions for class discussion, and getting initial ideas in play.

After the case study is being actively discussed per group, the instructor may see that some groups are too quiet or heading in the wrong direction. It is advantageous to correct this. Rarely, it may make sense to move people between groups, if some groups are not making sufficient progress or not getting along. At the end of the class, the instructor can ask specific teams for their solutions, particularly if they had brilliant ideas that should be shared, and/or can discuss the solution provided by the case study web site.

As an active learning exercise, students are given a small amount of credit for participating. If students miss the active learning exercise, they can submit it as homework. Due to the time constraints, perfect solutions may not occur during the lab time. However, having students think about the solution, and observe a good solution, helps them to assimilate the material. Often students come up with brilliant ideas, which have been incorporated into the official solution!

### *A. Results*

There are two questions when a course is taught: is the teaching effective, and do students appreciate their learning?

The real test of whether the teaching effectively 'helps students transition to the workplace', is whether students can work with a community partner on a real project afterwards. After a trial run with the case study, undergraduate students used the Workbook to work with small business management in our community. The instructor led the students for one visit to the community partner if students had IS/IT experience, or participated twice (of 6 visits) if they had no experience. The semester's work was rated highly by the community and students. Of our five community partner organizations that used the Workbook with student guidance, 100% were Very Satisfied with "The Quality of Students' Work". During our last year, students agreed (100%) or strongly agreed (28.6%) with the statement: "I felt that the community project I did through this course benefited the community partner's organization."

To obtain feedback from students about their learning, an independent evaluator performed a qualitative assessment with the students at the end of the course. The consensus on the case study was: "It was a good test drive". "Gave you a guideline for working with your partner". However, there was also a consensus that 'catching on' in the first few labs was difficult.

We also noticed that later labs had higher approval ratings than earlier labs. Our first four labs had an average 78% agreement rate to the statement: "I understood what was expected as part of the case study exercise, and it helped me to learn the material." During the next six labs this rate increased to 87.5%. (In both cases, all remaining students selected "Neither agree nor disagree".) To fix this, we currently start the case study as a class (and not groups). Volunteers read the case study out loud and discussion begins class-wide. Our initial approval rating then started out higher, with 93% 'agreeing' with the statement: "I understood what was expected as part of the case study exercise, and it helped me to learn the material."

## *V.* Acknowledgment

The development of the Small Business Security Workbook, lecture materials, and Health First Case Study was funded by the National Science Foundation (NSF) Course, Curriculum and Laboratory Improvement (CCLI) grant 0837574: Information Security: Audit, Case Study, and Service Learning. These materials are available at: www.cs.uwp.edu/staff/lincke/infosec. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

## VI. Conclusion

Security regulation should be an important aspect of security education, because students learn that security is not only a good idea, but also a requirement that organizations must adhere to. HIPAA is widely required, full-featured, and protects both privacy and security.

This case study teaches students to plan for security. The case study achieves an interdisciplinary aspect, by enabling students to experience multiple perspectives: the doctors', HIPAA regulation, IT and financial. Students gain practice with the case study, as for a real-world experience. It is effective, in that our students can lead real world community partners through security design.

## VII. References

[1] 14th Annual CSI Computer Crime and Security Survey Executive Summary, Computer Security Institute, GoCSI.com, Dec. 2009, p. 2.

[2] S. Lu and Y. Wang, "The Research and Practice of Case Teaching Method in Computer Curricula for Undergraduates", *Proc. 2009 4th International Conf. on Computer Science and Education*, IEEE, 2009, pp. 1460-1463.

[3] H. Wei, C. Xin, and H. Ying, "Non-computer Professional IT Education in the MBA Model", *The 5th International Conf. on Computer Science & Education*, 2010 IEEE, pp. 612-614.

[4] P. S. Chinowsky and J. Robinson, "Facilitating Interdisciplinary Design Education Through Case Histories", *1995 IEEE Frontiers in Education Conf.*, 1995 IEEE, pp. 4a3.6-4a3-9.

[5] G. Dhillon, *Principles of Information Systems Security*, John Wiley & Sons, Inc., 2007.

[6] ITGI, *IT Governance Using COBIT® and Val IT: Student Book, 2nd Ed.*, IT Governance Institute, www.isaca.org, Rolling Meadows, IL, 2007.

[7] ISACA, *Information Security Using the CISM® Review Manual and BMIS™: Caselets*, www.isaca.org, Rolling Meadows, IL, 2010.

[8] A. Katerinsky, H. R. Rao, and S. Upadhyaya, "Harsh Realities 101 - Augmenting Information Assurance with Legal Curricula" *Proc. 14th Colloquium for Information Systems Security Education (CISSE)*, www.cisse.info, 2010.

[9] N. P. Schembari, "An Active Learning Approach for Coursework in Information Assurance Ethics and Law", *Proc. 14th Colloquium for Information Systems Security Education (CISSE)*, www.cisse.info, 2010, pp. 1-8.

[10] S. J. Lincke, Susan, Small Business Information Security Workbook. Last Accessed on February 1, 2012 at http://www.cs.uwp.edu/staff/lincke/infosec/notes/SecurityWorkBook.doc

[11] S. J. Lincke, and T. Dorr, Health First Case Study. Last Accessed on February 1, 2012 at http://www.cs.uwp.edu/staff/lincke/infosec/notes/MedCaseStudy.doc

[12] T. Burri and S. J. Lincke, "Security Planning for Small Businesses: A Service-Learning Course", *IEEE Frontiers in Education*, 2011.

[13] ISACA, *CISA Review Manual 2010*, Arlington Heights IL. DOI=http://www.itgovernance.co.uk/products/1403, 2009.

[14] ISACA, *CISM Review Manual 2010*, Arlington Heights IL. DOI=http://www.itgovernance.co.uk/products/1402, 2009.

[15] Carlene Dalgleish, "HIPAA Compliance" (Course Notes), Triton College, River Grove IL, 2009.

[16] Joanna Lyn Grama, *Legal Issues in Information Security*, Jones & Bartlett Learning, 2010, pp. 142-179.

[17] Pabrai, U. A., *The Art of Information Security*, ECFirst.com, 2005, pp. 159-170.