# Implementation of HIPAA Certification and Training Guidelines for Healthcare Organizations Structured after the IS 2002 Model Curriculum

David Sweatt
Children's and Women's Hospital
University of South Alabama
Mobile, AL 36604
dsweatt@usouthal.edu

Herbert E. Longenecker, Jr.
and
Robert B. Sweeney
School of Computer and Information Sciences
University of South Alabama
Mobile, AL 36688
hlongenecker@usouthal.edu
bsweeney@usouthal.edu

## Abstract

Every person in a healthcare organization is a member of the Health Insurance Portability and Accountability Act of 1996 workforce, and as such must become HIPAA aware and compliant. Ensuring broad HIPAA compliance requires an effective, flexible, scalable, and comprehensive awareness, training, and certification program. In this paper a comprehensive proposal is advanced to identify work force stratifications, according to stair-stepped cognitively defined levels compatible with work force responsibilities and, therefore, educational requirements. A parallel structure to the IS'2002 Curriculum Model is presented. The HIPAA model begins with exit skill definitions, the equivalent of courses, cognitively defined learning units, and a skill-learning unit map suitable for implementation of assessment and certification requirements. This is referred to as a HIPAA Curriculum. The primary goal of the proposed HIPAA Curriculum is to achieve competency in the defined HIPAA skill set for each identifiable workforce level.

**Keywords:** Administrative Simplification, HIPAA Security, HIPAA Privacy, healthcare workforce certification

### 1. INTRODUCTION

Protecting the confidentiality, integrity and availability of patient data has always been vital, but now its federal law. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 established specifications for the transmission, storage, disclosure and use of protected health information that healthcare organizations must meet. Compliance with HIPAA means more than filling out privacy disclosure forms. Rather, significant changes in IS and IT functions, business transactions, and workforce member behaviors must be accomplished and documented.

Compliance with HIPAA requires delivering effective, ongoing communication and education to the organization workforce. Compliance also necessitates the close participation and consultation of the organization's Information Technology (IT) department. It is the assertion of this implementation that measurable workforce competency in the skills necessary to achieve and maintain HIPAA compliance can be attained through an awareness and training program that is developed using the framework and methodology of the IS 2002 Model Curriculum as a template.

## 2. HIPAA EXPECTATIONS

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a set of regulations and provisions for the healthcare industry from the US Department of Health and Human Services (HHS). Although HIPAA was passed into law in many years ago, it is only recently that major components of the Act have gone into effect.

At its top most level, HIPAA can be divided into five relatively unrelated areas. HIPAA Administrative Simplification consists of five general areas (Bowen, 2004) including Security, Privacy, Electronic Data Interchange (EDI) transaction standards, Identifiers for unique designations and Code Sets for healthcare services. It is the Administrative Simplification provisions, hereafter referred to as HIPAA, which this project will focus on (Fig. 1).

HIPAA designates how healthcare organizations should disclose, use, store, protect and transmit individually identifiable data related to patients and their care, commonly referred to as Protected Health Information (PHI). The regulations for Code Sets, Identifiers and EDI transactions pertain to the structure and transmission of Protected Health Information. HIPAA Privacy regulations commonly referred to as the Privacy Rule, address the use and disclosure of PHI. HIPAA Security regulations, commonly referred to as the Security Rule, deal with storage and protection of Electronic Protected Health Information (EPHI), which includes all PHI in electronic form.

Ultimately, HIPAA seeks to safeguard the confidentiality, integrity and availability of protected health information and simplify the administrative overhead associated with these goals.

HIPAA compliance must be achieved by three main types of healthcare organizations, also known as Covered Entities (CE). The three types of covered entities are health care providers (includes hospitals, clinics and private practices), health plans (payer organizations such as insurance companies) and healthcare clearinghouses (service organizations). Compliance with HIPAA regulations must be met by covered entities at the organization level as well as the employee workforce level. The Covered Entity accomplishes this through the adoption of HIPAA compliant code sets, identifiers and data interchange transactions along with comprehensive policies and procedures that address the Privacy and Security concerns outlined for HIPAA Administrative Simplification in the Federal Register.

Although the vast majority of HIPAA compliance deadlines have passed, organizations continue to struggle to become compliant. The most recent HIPAA compliance deadline, the Security Rule, passed on April 21 2005. Survey results from January 2005 that include 400 healthcare organizations (80% of respondents were healthcare providers while 20% were healthcare payers) reveal that only 30% of payers and only 18% of providers indicate that they are currently compliant with the HIPAA Security regulations (Phoenix, 2005). The Phoenix - Healthcare Information and Management Systems Society (HIMSS) Survey also reports that 78% of providers and 90% of payers indicated that they are compliant with the Privacy Rule (Phoenix, 2005), a deadline that passed April 2003. Finally, the survey reports that compliance toward HIPAA transactions and code sets, a deadline that passed October 2002, has improved over the last six months – 73% of providers and 70% of payers indicate compliance – up from 65% and 62% respectively (Phoenix, 2005).

## 3. RESPONSIBILITY OF THE IT DEPARTMENT IN HIPAA COMPLIANCE

Information Technology is a major underlying component of HIPAA compliance, and as such the IT department plays several key roles within the activities of HIPAA compliance for an organization. Two of the five general areas of HIPAA (Fig. 1), Security and EDI Transactions, rely heavily on the functions of the IT department. Compliance could not be achieved in these areas without the IT department's expertise in computer hardware and software security, networking security, and data transmissions and communications. Enacting and enforcing the standards for Unique Identifiers and Code Sets for HIPAA (Fig. 1) would be difficult without the IT department as these standards generally exist within and between systems software. In addition, the IT department is the natural choice for core HIPAA compliance activities such as developing and executing emergency contingency plans for computing systems, designing and implementing backup and recovery schemes, performing risk assessment of computing assets, providing and implementing recommendations for changes that arise from risk mitigation, and providing an effective and efficient system for documenting HIPAA compliance activity. Finally, because HIPAA security is essentially a specialized niche of the broader IT security field, a workforce member seeking a leadership role in HIPAA security could, with appropriate training in HIPAA skills and knowledge, smoothly make the transition from IT security professional to HIPAA Security Officer.

## 4. HIPAA APPLICABILITY AND ASSURANCE THROUGH EDUCATION

HIPAA mandates that covered entities designate HIPAA compliance officers within the organization. The HIPAA Privacy Officer is responsible for implementing and enforcing policies and procedures that address the HIPAA Privacy Rule. Likewise, the HIPAA Security Officer is responsible for implementing and enforcing policies and procedures that address the HIPAA Security Rule.

The HIPAA compliance officers must plan and implement a system to document all HIPAA compliance activities. All covered entities will benefit from the adoption of an information model for HIPAA related activities and data. The model should describe the underlying entities, relationships and processes of HIPAA regulations and compliance activities.

Peggy Fung states that "comprehensive, updated security documentation is a keystone of good security management" (Fung, 2003). Fung notes that flat, text based documentation is not an effective solution for managing such complex information security problems. "It has been suggested that a security officer's workstation, with a database and GUIs, may present a more effective form of security documentation" (Fung, 2003). Fung continues, "Such a tool requires a well developed model of the information system and (…) a standardized means of representing security entities."

Once the compliance foundations are in place at the organizational level, each workforce member within the organization must be trained to function within the HIPAA regulations. The HIPAA officers are required to ensure that all workforce members are in compliance. Bringing the workforce to a state of compliance and ensuring continued compliance can be achieved through a solid education program. Furthermore, "all covered entities will be required to develop, maintain and demonstrate their efforts to communicate build awareness and educate their employees" (WEDI, 2001).

Identifying an organization information model for HIPAA as mentioned above is a crucial part of a foundation for implementing a HIPAA workforce education program. HIPAA education should yield competency for all levels of the workforce through "a multidimensional approach for training geared towards various sectors within the workforce" (Upham, 2001). "Avoid 'one size fits all training' " Upham says is one of several steps organizations should take to achieve "successful HIPAA training".

## 5. HIPAA TRAINING AND AWARENESS PROGRAM

Randa Upham outlined a question and answer approach to defining a HIPAA education program.

Who should be trained?

What information should be included?

What is the best method? (Upham, 2001),

Upham identified several criteria that help answer the question of who. Her conclusion was that all workforce members associated with a covered entity should be trained at some level for HIPAA. An education model for HIPAA should identify all levels of workforce member within the organization.

Upham answered "What should be included?" by describing several training areas including "Privacy regulations" and "Security regulations" and "mandated training" vs. "specific needs" for all workforce members. Mandated training would include the knowledge and skills specified in the HIPAA regulations whereas specific needs refer to those organization specific policies and procedures.

To answer the question "What is the best method?" Upham described a comprehensive mix of "traditional classroom instruction", "computer based training", "supervisory sessions" and third party "distance learning" (Upham, 2001) where each delivery method is used for specific training situations. She felt that for computer assisted learning and examination, care should be taken when selecting an off the shelf product or designing a custom system. Many organizations are choosing computer based approaches to meet compliance with large workforces (Upham, 2001). "Computer-assisted assessment (CAA) is often applied out of a desire to counter the increasing time demands on staff while still delivering an acceptable educational experience" (Joy, 2002). Joy warns however that the "most time intensive stage of using CAA is when it is being introduced – long term gains in efficiency are often at a cost of short term effort".

Continuing education is an important requisite for compliance. "A formal, ongoing enterprise-wide training program" is needed (Gue, 2003). "A one time education initiative … is not sufficient". In addition, a HIPAA education program must remain flexible and relevant. "As new regulations are published or internal policies amended, continuing training must be applied" (Gue, 2003).

The National Institute of Standards and Technology has outlined a life cycle approach to establishing a HIPAA training program. Key activities of the life cycle include (Bowen, 2004):

Conduct a training needs assessment

Develop and approve a training strategy and plan

Develop appropriate awareness and training content

Implement the training plan

Monitor and evaluate the training plan

NIST also explains that security awareness and training should be focused on the organization's entire user population (Wilson, 2003). "An awareness and training program is crucial in that it is the vehicle for disseminating information that users, including managers, need in order to do their jobs". An organization's education program ensures compliance and competency.

Ultimately, the goal of a HIPAA training program is workforce certification. The program must ensure that all workforce members function appropriately within the confines of HIPAA regulations. "Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them" (Wilson, 1998).

## 6. THE IS'97 AND IS'2002 MODEL CURRICULA

The goal of IS'97 (Longenecker, 1995; Davis, 1997) and IS'2002 (Gorgone, 2002) is to produce graduates who are confident and competent in executing job-entry level skills. The curriculum is broken into units called curriculum areas which frame the curriculum. The initial area is the first exposure for learners to the discipline. The exit areas are responsible for conferring the desired exit level skills. The intermediate areas develop knowledge necessary to express the discipline, and to prepare learners for the finishing areas. Courses define each area, and are specified by learning units which describe cognitive performance criteria for each course. Skills are attained piece-wise, that is, a little at each level (learning unit) of the curriculum. From initial to exit levels, successive skills define a skill thread. Each of these threads

may be assessed anywhere along the thread.

## 7. APPLICATION OF THE IS MODEL TO HIPAA EDUCATION AND CERTIFICATION

The underlying structure of the proposed HIPAA education model (Fig. 2), or curriculum, is patterned after the structure of the IS 2002 Curriculum (Gorgone, 2002). The methodology used to identify and develop the elements of the HIPAA curriculum are parallel to the IS 2002 Model.

It is our proposition that sufficient skill will be attained after completing courses associated with each HIPAA Compliance Curriculum area such that 1) A component of the workforce will have been satisfied after completing a given course, and 2) Completion of the curriculum area is a sufficient prerequisite to the next area.

In the HIPAA Compliance Curriculum, three curriculum areas are identified along with ten courses. Dotted lines are used to show the element of the work force satisfied subsequent to completing a given course.

Each course is defined by a set of learning units. Each element of knowledge and skill within the HIPAA learning unit is designated with an exit competency level that is based on the IS 2002 Model's Depth of Knowledge Metrics (Gorgone, 2002), which in turn are based on Bloom's Taxonomy for cognitive learning. The original Bloom Taxonomy "characterizes problems by six levels (knowledge, comprehension, application, analysis, synthesis and evaluation)" (Joy, 2002), whereas the IS 2002 Model specifies four curriculum competency levels (awareness, literacy, comprehension and application) (Gorgone, 2002). Comparatively, the National Institute for Standards and Technology (NIST) categorizes three levels of competency in Information Technology security training (awareness, training and education) (Wilson, 1998).

Based on the HIPAA Administrative Simplification specifications and standards from the Federal Register and the publications of the National Institute of Standards and Technology (the Mandated Training component (Upham, 2001)), and the policies and procedures for HIPAA Privacy and Security for the University of South Alabama Hospitals (the Specific Needs component (Upham, 2001)), a comprehensive skill set was identified. (Table 1) illustrates the skill set.

We derived courses from a detailed analysis of expectations of each level of workforce member to be trained. (Table 2) provides a brief description of the identified courses.

Likewise, detailed presentation goals and objectives were developed for each course comprising the HIPAA compliance learning units. The skills (Table 1) were mapped to the learning units in order to determine precisely how the exit skills were to be developed during training sessions. We have completed a similar mapping, and have specified sets of Skill-LU pairs to evaluate the competency of workforce course graduates. A sample Skill-LU pair for a course is illustrated in (Table 3).

The Center for Computing Education Research (CCER) developed assessment exams (McKell, 2004) for universities based on Skill—Learning Unit (LU) pairs. An adequate number of questions were developed to evaluate not only the exit level skills, but the learning units as well. The Institute for Certification of Computing Professionals (the ICCP) awards the Information Systems Analyst (ISA) Certification to graduates who pass this examination. We plan to implement the HIPAA Compliance Exam(s) in a manner that they could be used by the CCER, and conceivably the ICCP.

## 8. CONCLUSIONS

It is proposed that the development of a HIPAA education and training curriculum based on a proven model will enable us to produce certifications (Table 4) for each workforce level of accomplishment. The adoption of certifications would enable documentation of HIPAA compliance efforts and potentially lend itself to the establishment of a national standard.

## 9. REFERENCES

Bowen, Pauline, Arnold Johnson, Joan Hash, Carla Dancy Smith, Daniel Steinberg. Information Security, an Introductory Resource Guide for Implementing the Health Insurance Portability and

Accountability Act (HIPAA) Security Rule. National Institute of Standards and Technology. NIST Special Publication 800-66, Draft. May 2004.

Fung, P., L Kwok, D Longley. "Electronic Information Security Documentation." Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 – Volume 21. ACM Digital Library.

Gorgone, John T., Gordon B. Davis, et al. IS 2002, Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems. Association for Information Systems. 2002.

Gue, D'Arcy Guerin. Training – The First and Last Word in Privacy Compliance. HIPAA Advisory, Phoenix Health Systems, October 2003.

Joy, Mike, Boris Muzykantskii, Simon Rawles, Michael Evans. "An Infrastructure for Web-Based Computer-Assisted Learning." Journal on Educational Resources in Computing (JERIC). Vol. 2, Issue 4, December 2002. ACM Digital Library.

McKell, L.J., J.H. Reynolds, H.E. Longenecker, J.P. Landry, H. Pardue. "Integrating Program Evaluation and a New Certification for Information Technology Professionals." SITITE. ACM Digital Library. October 2004.

US Healthcare Industry HIPAA Compliance Survey Results: Winter 2005, HIPAA Advisory, Phoenix Health Systems - Healthcare Information Management Systems Society (HIMSS), January 5-20, 2005.

Upham, Randa. "Educating the Organization." Health Management Technology. December 2001.

Strategic National Implementation Process – Security and Privacy Workgroup – Awareness Training and Education. Workgroup for Electronic Data Interchange, December 2001.

Wilson, Mark, Dorothea E. de Zafra, Sadie I. Pitcher, John D. Tressler, John B. Ippolito. Information Technology Security Training Requirements: A Role and Performance Based Model. National Institute of Standards and Technology. NIST Special Publication 800-16, April 1998.

Wilson, Mark, Joan Hash. Building an Information Technology Security Awareness and Training Program. National Institute of Standards and Technology. NIST Special Publication 800-50, October 2003.

# Appendix

**Figure 1: Administrative Simplification in Relation to All Components of HIPAA**

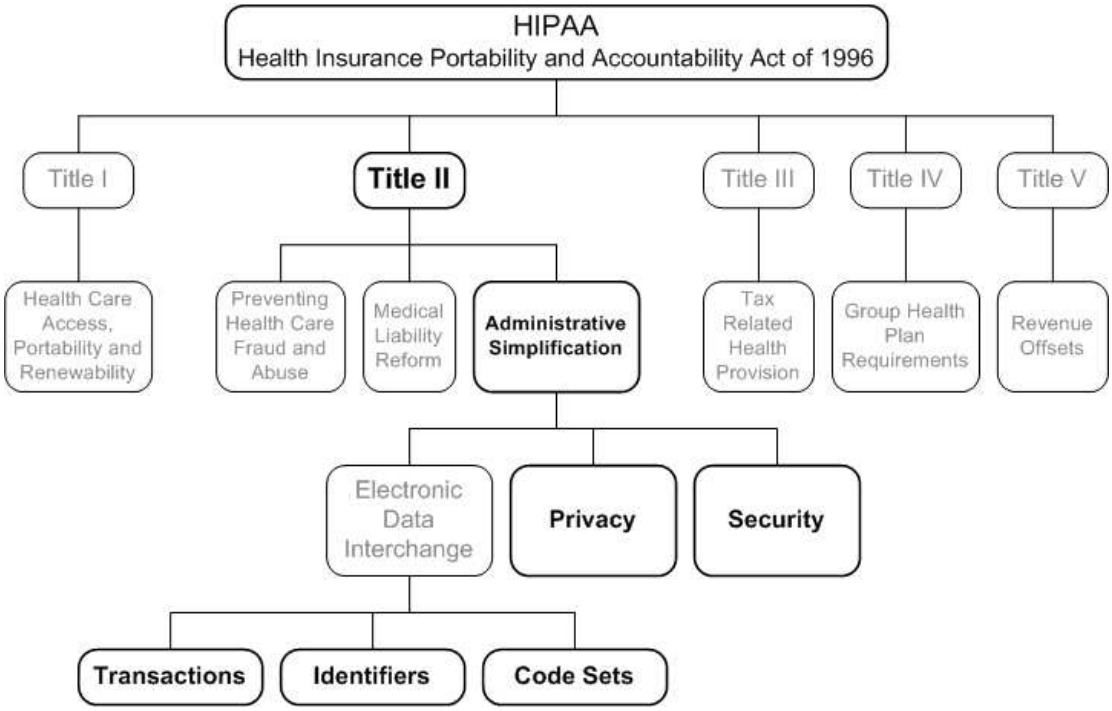


**Figure 2: Proposed HIPAA Compliance Curriculum**

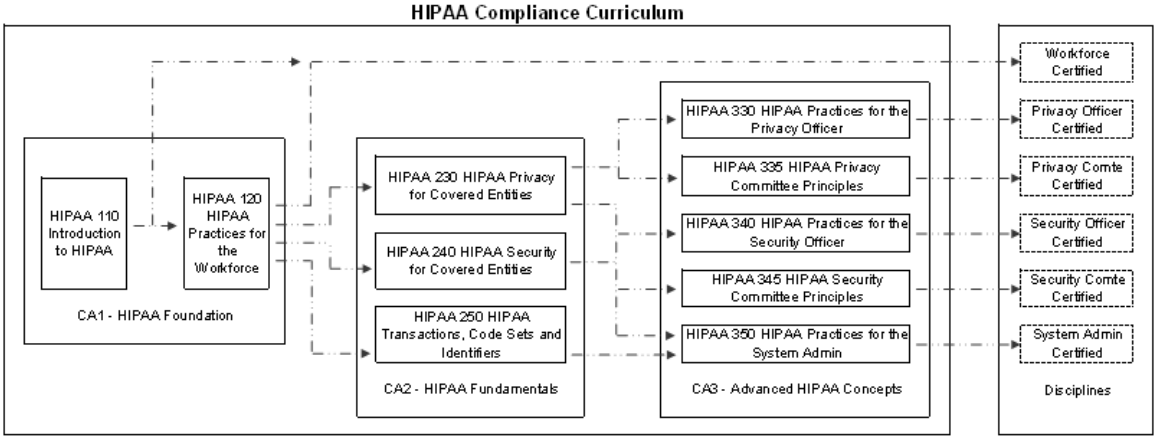


**Table 1: HIPAA Skills Set**

| |
|---|
| **1.0 Security Rule Management** |
| **1.1 Managing Administrative Standards** |

| | |
|---|---|
| 1.1.1 Security Management Processes | identification of risks, threats, and vulnerabilities, risk analysis, risk management, risk mitigation, establish sanction procedures, develop violation reporting process, information system activity review |
| 1.1.2 Managing Security Responsibilities | identify security officer responsibilities, identify security committee member responsibilities, develop and implement Security Plan, establish policies and procedures for administrative, physical and technical standards |
| 1.1.3 Workforce Security Practices | workforce authorization, establish job responsibilities, minimum necessary procedures, task assignment process, restricting access, establish termination procedures |
| 1.1.4 EPHI Access Management | determine access criteria, establish information access standards, examine security measures |
| 1.1.5 Awareness and Training Implementation | conduct training needs assessment, develop training strategy, establish training program, develop training content, establish system of alerts |
| 1.1.6 Security Incident Procedures | incident identification, incident reporting, incident investigation, incident response, incident resolution |
| 1.1.7 Contingency Planning | data backup planning, disaster recovery procedures, emergency mode operations, contingency testing and revision, data criticality analysis |
| 1.1.8 Security Evaluation Practices | establish evaluation standards and procedures, develop standards and measures for security evaluation, conduct security evaluations |
| 1.1.9 Managing Business Assoc. Contracts | identify business associates, establish or modify contracts, develop measures for contract performance |
| **1.2 Managing Physical Standards** | |
| 1.2.1 Managing Facility Access | physical security analysis, identify corrective measures, develop facility security plan, establish access control procedures, establish contingency operation procedures |
| 1.2.2 Workstation Use Procedures | identify workstation types and functions, identify performance and security issues, analyze physical attributes and workstation environment, establish workstation security procedures |
| 1.2.3 Managing Workstation Security | identify workstation physical access methods, analyze access risks, identify physical safeguards, develop physical security procedures |
| 1.2.4 Device and Media Management | evaluate methods of disposal, develop reuse procedures, develop and maintain media documentation, establish backup procedures for media |
| **1.3 Managing Technical Standards** | |
| 1.3.1 Access Control Management | identify and analyze access needs of all users, determine access control needs, enforce unique identifiers, develop access control procedures, implement access controls |
| 1.3.2 Audit Control Management | audit policies, audit procedures, implement hardware mechanisms, implement software mechanisms, record and examine activity |
| 1.3.3 EPHI Integrity Management | integrity policies, integrity procedures, improper alteration or destruction protection, mechanisms to authenticate EPHI |
| 1.3.4 Authentication Management | person/entity authentication policies, person/entity authentication procedures |
| 1.3.5 Managing Transmission Security | integrity control, encryption, technical security measures, unauthorized access, appropriate mechanisms |
| **2.0 Privacy Rule Management** | |
| **2.1 Managing Administrative Standards** | |

| | |
|---|---|
| 2.1.1 Privacy Management Processes | ensure confidentiality, integrity, and availability of PHI, identify covered entities, establish sanction procedures, develop violation reporting process |
| 2.1.2 Managing Privacy Responsibilities | identify privacy officer responsibilities, identify privacy committee member responsibilities, develop and implement Privacy Plan, establish policies and procedures, develop documentation standards |
| 2.1.3 PHI Access Management | determine access criteria, establish information access standards, examine privacy measures |
| 2.1.4 PHI Authorization Management | identify workforce PHI needs, establish authorization procedures |
| 2.1.5 Managing Info. Use and Disclosure | establish PHI use procedures, establish PHI disclosure procedures |
| 2.1.6 Awareness and Training Implementation | conduct training needs assessment, develop training strategy, establish training program, develop training content, establish system of continued awareness |
| 2.1.7 Privacy Incident Procedures | incident identification, incident reporting, incident investigation, incident response, incident resolution |
| 2.1.8 Minimum Necessary Practices | establish job responsibilities, minimum necessary procedures, task assignment process, restricting access, establish termination procedures |
| 2.1.9 Managing Business Associate Contracts | identify business associates, establish or modify contracts, develop measures for contract performance |
| 2.1.10 Patient Rights Management | identify patient rights to PHI, establish patient information access procedures, managing patient information requests |
| 2.1.11 Safeguarding PHI | establish procedures for handling, distributing, storing and disposing of PHI, develop safeguards for PHI use and disclosure by telephone |

**Table 2: Proposed HIPAA Courses**

| |
|---|
| **HIPAA 110 Introduction to HIPAA** |
| HIPAA concepts and practices are introduced. Protected Health Information and its risks are identified. Incident reporting and patient rights are stressed. The concepts of PHI use, disclosure and authorization are explained and demonstrated. |
| **HIPAA 120 - HIPAA Practices for the Workforce** |
| HIPAA concepts are reinforced and expanded upon. Information and facility access practices are introduced. The Privacy Rule and Security Rule are introduced. Skills for safeguarding assets, applications and media are developed. |
| **HIPAA 230 - HIPAA Privacy for Covered Entities** |
| HIPAA Privacy policies and procedures adoption is introduced. Business Associate Agreements are introduced. Key responsibilities of the HIPAA Privacy Officer are furthered. Training and Awareness program goals are discussed. Patient Rights management is furthered. Documentation practices are explained and demonstrated. Disclosure of de-identified data is explained. |
| **HIPAA 240 - HIPAA Security for Covered Entities** |
| HIPAA Security policies and procedures adoption is introduced. Business Associate Agreements are introduced. Key responsibilities of the HIPAA Security Officer and the system admin are furthered. Principles and procedures of risk management are introduced. Training and Awareness program goals are discussed. Security contingency plans are introduced. Documentation practices are explained and demonstrated. Security evaluation and auditing are introduced. |
| **HIPAA 250 - HIPAA Transactions, Code Sets and Identifiers** |
| Data transaction HIPAA standards and industry protocols are explored. HIPAA standard code sets are introduced. HIPAA standard identifiers are introduced. Integrating new EDI standards with existing systems is explored and demonstrated. |
| **HIPAA 320 - HIPAA Practices for the System Admin** |

| |
|---|
| Application of the principles and processes of information access management are developed. Implementing a facility security plan is explained. Managing contingency operations is explored and demonstrated. Executing workforce and workstation monitoring and oversight are explained and demonstrated. Implementation of audit control mechanisms and processes are explored. Information transmission security principles are introduced. Executing a risk management program is demonstrated. |
| **HIPAA 330 - HIPAA Practices for the Privacy Officer** |
| Interpretation of the Privacy Rule is completed. Conceptualization and implementation of Privacy policies and procedures are developed. Implementation of documentation best practices is completed. Workforce evaluations and oversight activities are introduced and demonstrated. Incident management and workforce sanctions are explained and demonstrated. Implementing and managing a Privacy training and awareness program are explored and demonstrated. |
| **HIPAA 335 - HIPAA Privacy Committee Principles** |
| Interpretation of the Privacy Rule is completed. Conceptualization, implementation and revision of Privacy policies and procedures are developed. Privacy incident mitigation is explored. |
| **HIPAA 340 - HIPAA Practices for the Security Officer** |
| Interpretation of the Security Rule is completed. Conceptualization and implementation of Security policies and procedures are developed. Implementation of documentation best practices is completed. Workforce evaluations and oversight activities are introduced and demonstrated. Incident management and workforce sanctions are explained and demonstrated. Implementing and managing a Security training and awareness program are explored and demonstrated. Managing audit control is explored. Executing a risk management program is explored and demonstrated. |
| **HIPAA 345 - HIPAA Security Committee Principles** |
| Interpretation of the Security Rule is completed. Conceptualization, implementation and revision of Security policies and procedures are developed. Security incident mitigation is explored. |

**Table 3: Sample Learning Unit Goals, Objectives and Skills Map for a Course**

| **HIPAA 110 Introduction to HIPAA** | | | |
|---|---|---|---|
| 1 | LU Goal | LU Objectives (SWBAT) | Skills Map |
| | To introduce the concepts and definitions of HIPAA | Define HIPAA Privacy terms | 2.1.1 Privacy Management Processes |
| | | Define HIPAA Security terms | 1.1.1 Security Management Processes |
| | | Explain the purpose and goals of HIPAA | 1.1.3 Workforce Security Practices<br>2.1.11 Safeguarding PHI |
| | | Differentiate between the HIPAA Rule and a HIPAA Plan | 1.1.2 Managing Security Responsibilities<br>2.1.2 Managing Privacy Responsibilities |
| | | List the entities covered by HIPAA | 2.1.1 Privacy Management Processes |
| 5 | To explain the fundamentals of PHI identification | Differentiate between PHI and EPHI | 1.1.1 Security Management Processes |
| | | Identify PHI | 2.1.7 Privacy Incident Procedures |
| | | Identify EPHI | 1.1.6 Security Incident Procedures |
| | | List and explain PHI and EPHI Risks | 1.1.1 Security Management Processes |
| 10 | To develop the ability to report privacy and security incidents | Explain the incident reporting process | 2.1.7 Privacy Incident Procedures<br>1.1.6 Security Incident Procedures |
| | | Explain the responsibilities and importance of incident reporting | 2.1.7 Privacy Incident Procedures<br>1.1.6 Security Incident Procedures |
| | | Submit an incident report | 2.1.7 Privacy Incident Procedures<br>1.1.6 Security Incident Procedures |
| 15 | To relate the importance of patient rights and PHI use and disclosure | List and explain basic HIPAA patient rights | 2.1.10 Patient Rights Management |
| | | Discuss proper PHI disclosure and recognize improper use | 2.1.5 Managing Information Use and Disclosure |
| 20 | To introduce the concepts and | Explain the implications of authorization for access to PHI | 2.1.4 PHI Authorization Management<br>1.3.1 Access Control Management |

| | | | |
|---|---|---|---|
| | processes of PHI authorizations and notifications | and EPHI | |
| | | Recognize Privacy and Security notifications | 1.1.5 Awareness and Training Implementation<br>2.1.6 Awareness and Training Implementation |
| | | Recognize potential unauthorized attempts to access PHI or EPHI | 2.1.4 PHI Authorization Management<br>1.1.3 Workforce Security Practices |
| 25 | To explain best practices for safeguarding PHI | Discuss use and disclosure protective measures | 2.1.5 Managing Information Use and Disclosure<br>2.1.11 Safeguarding PHI |
| | | Recognize potential EPHI devices and media | 1.2.4 Device and Media Management |
| | | Discuss device and media safeguarding practices | 1.2.2 Workstation Use Procedures<br>1.2.3 Managing Workstation Security |
| 30 | To introduce the responsibilities of the HIPAA workforce and Officers | Explain the responsibilities of the workforce member | 2.1.8 Minimum Necessary Practices<br>1.1.3 Workforce Security Practices |
| | | Describe the responsibilities of the system admin, security officer and privacy officer | 1.1.2 Managing Security Responsibilities<br>2.1.2 Managing Privacy Responsibilities |

**Table 4: HIPAA Certifications**

| Organization Role | Certification | Certification Name |
|---|---|---|
| Workforce Level 1 | CHW | Certified HIPAA Workforce |
| Workforce Level 2 | CHWA | Certified HIPAA Workforce Advanced |
| System Administrator | CHSA | Certified HIPAA System Administrator |
| Privacy Officer | CHPO | Certified HIPAA Privacy Officer |
| Privacy Committee Member | CHPC | Certified HIPAA Privacy Committee |
| Security Officer | CHSO | Certified HIPAA Security Officer |
| Security Committee Member | CHSC | Certified HIPAA Security Committee |