A HIPAA Strategy for Dental Schools

Rosemary Walker, D.D.S., M.B.A., M.S.

Abstract: Certain health care organizations, including dental schools, should be readying themselves to comply with the numerous requirements described within the administrative simplification section of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The intent of administrative simplification is to streamline the management of health care transactions while protecting the privacy of certain written, oral, and electronic patient information. There are no field-tested plans for implementing the law because only recently has the health care industry begun to respond to the multitude of requirements. It is essential that each organization create a customized compliance plan that best fits its structure and needs. The purpose of this paper is to propose a five-stage theoretical strategy that could assist a dental school in achieving HIPAA compliance. The first stage involves the selection of a HIPAA task force. The second stage selects the applicable HIPAA requirements, determines the current states of confidentiality and security, manages the electronic transactions standards, and composes a gap analysis. The third stage examines risk analysis and management. The fourth stage encompasses technical modifications, policies and procedures, legal input, and training. The fifth stage addresses the maintenance of the implementation.

Rosemary Walker is Clinical Assistant Professor at the University of Illinois at Chicago College of Applied Health Sciences. Direct correspondence to her at the University of Illinois at Chicago, College of Applied Health Sciences, School of Biomedical and Health Information Sciences, 1919 W. Taylor M/C 530, Chicago, IL 60612-7249; 312-996-5112 phone; rwalke7@uic.edu.

Key words: HIPAA, dental school, academic medical center, strategy, risk analysis, gap analysis, privacy, security, electronic transactions

Submitted for publication 12/19/02; accepted 4/8/02

The health care industry has long recognized the need to standardize the collection, exchange, and use of electronic health/health care-related information and demographic data. But although the demand for standardization was present, it had not been actualized. Finally, Congress decided that government intervention was the most expedient means of implementing industry standards and addressed this issue in the Kennedy-Kassebaum Bill, also known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA’s purpose is broad-spectrum: improve portability and continuity of health insurance coverage in the group and individual markets; combat waste, fraud, and abuse in health insurance and health care delivery; promote the use of medical savings accounts; improve access to long-term care services and coverage; and simplify the administration of health insurance.1

The section of HIPAA that has caused concern throughout the health care industry is “Administrative Simplification” under Title II, Subtitle F. This section was designed to establish standards and requirements for the electronic transmission of certain transactions with a resultant improvement in the efficiency and effectiveness of the health care system.1 Affected are the “covered entities”: health plans, health care clearinghouses, and health care providers who transmit patient information via the electronic standards established by HIPAA. Congress perceived that the key to administrative simplification was protection of the privacy and confidentiality of personal health information. Therefore, the first pack-
The Department of Health and Human Services (HHS) is orchestrating implementation of the simplification goal. It began by establishing “proposed” rules for electronic transactions, privacy, security, national health provider identifiers, and national employer identifiers. HHS will ultimately post rules for health plan identifiers, individual identifiers, claims attachment transactions, and first report of injury transactions.

After publishing the first set of proposed rules, HHS considered and then integrated comments from the health care industry. The department began releasing “final” rules, starting with electronic transactions, on August 17, 2000. Its implementation deadline is October 16, 2002. The final privacy rule was published December 28, 2000, and is to take effect April 14, 2003. At the time this article was written, only the final rules for electronic transactions and privacy had been published.

Each rule when posted in final form has a compliance deadline that is usually two years and sixty days from the date of posting. The current final rules digress from this required deadline. Due to an administrative problem, privacy rule compliance was shifted an additional sixty days to April 14, 2003. The electronic transactions deadline may be extended an additional year to October 16, 2003, if a compliance extension plan is submitted to HHS by October 16, 2002. This plan must adhere to the conditions established in the Administrative Simplification Compliance Act (www.aha.org/hipaa/resources/Content/HR3323.pdf).

A final rule may be modified any time in the first year after a rule or implementation specification has been initially adopted if HHS “determines that the modification is necessary to permit compliance with the standard or implementation specification.” After the first year, a rule may be modified not more than once annually. At the time this article was published, proposed modifications to the final privacy had just been published on March 27, 2002. These modifications are open to public comment for a thirty-day period.

The electronic transactions final rule stipulates standards for eight electronic data interchange (EDI)-based electronic transactions and code sets. Dental schools will generally only use the Code on Dental Procedures and Nomenclature (CDT-3). The final privacy rule establishes requirements and general rules for the management of protected health information (PHI). In the proposed security rule, both requirements and possible strategies for implementation are provided. The remaining published proposed rules contribute possibilities for a national employer identifier and a national provider identifier.

The law establishes sanctions to uphold the rules, but precludes the possibility of a school being selected for random inspection. While the Office of Civil Rights is responsible for privacy rule infractions, no agency has been designated to enforce the other rules. Guidance will be provided through an enforcement rule that will be posted in the near future.

Further information on the history or the rules can be attained at such online sites as www.hipaadvisory.com, aspe.hhs.gov/admsimp, and www.ada.org/prof/prac/issues/topics/hipaa/index.html.

**HIPAA and the Dental School**

Health care organizations are reworking their clinical, technological, and administrative processes to address the requirements established by HIPAA. HIPAA will compel many organizations to modify certain aspects of clinical patient management, but academic medical centers, such as dental schools, are faced with additional challenges created by their research and education missions. These schools will find, as hospitals and insurance companies are discovering, that HIPAA compliance requires an investment in time and resources. Additionally, the lack of benchmarks and experts, as well as the absence of several of the final rules, complicates the situation.

Academic medical centers have an advantage that facilitates HIPAA compliance: a well-educated, hard-working workforce who have traditionally served as innovators in health care and play an active role in national health care policy development. Despite this advantage, these centers are faced with potential barriers to HIPAA compliance that often are inherent to this type of organization, such as a complex organizational/governance structure and unclear/nonexistent reporting lines. Information system users extend beyond school employees to nonemployees such as predoctoral and postdoctoral students. Additionally, a decentralized school system that is guided by numerous committees may have an inability to act cohesively and expeditiously.
Managing compliance with HIPAA requirements necessitates the cooperation of everyone who is responsible for PHI within a health care organization. Favorable outcomes and sustained success are the results of a unified effort that is strongly supported by the top echelon of the school.

Strategy for HIPAA Compliance

The key word in the rules that drives any HIPAA compliance strategy is “reasonable.” Its importance is emphasized by the word’s use 265 times within the initial final privacy regulation and preamble. Each school determines what is reasonable for its compliance strategy. Implementation is not a lock-step process for all organizations; it is intentionally scalable. HIPAA provides a framework of requirements for methods of implementation that are dictated by the needs and capabilities of an individual school. From a technological standpoint, the law remains neutral, not specifying particular hardware or software.

HHS did not intend to create new and/or impossible obstacles for health care organizations. A school should already have a semblance of compliance in regard to the privacy and security requirements, adhering to the American Dental Association’s “Principles of Ethics and Code of Professional Conduct” that have stated for more than twenty years that dentists should protect the confidentiality of patients’ records. In regard to electronic transactions, schools are currently dealing with a multitude of formats; HIPAA wants to limit this to the minimum necessary.

Approaches for gaining compliance are being developed by other health care organizations. Dental schools should also devise strategies for implementation dependent upon their individual business practices. There are no proven strategies because HIPAA compliance is in its infancy. This proposed strategy is based on my own approach to addressing HIPAA requirements within a dental school.

The First Stage: Select a HIPAA Task Force

The task force members are the champions for the initiative, generating and supporting actions that are required to achieve compliance. To emphasize the importance of this undertaking, members should be appointed by the dean of the school. As the only positions specifically designated by HIPAA are privacy officer and contact person, there need not be a set number for this group. Possibilities include an assistant/associate dean, a security officer, a contact person, a sanctions official, a training officer, and a representative of each of the following: the graduate programs, the general dentistry department, the undergraduate specialty faculty, satellite clinics, and support staff. Subcommittees can be appointed as needed by the members. Legal representation should be available for consultation.

The Privacy Officer

According to HIPAA, the privacy officer serves as “a center point of accountability.” This officer’s major duties are to develop and implement privacy policies and procedures and also to guarantee compliance. He or she will be guided by the HIPAA-specified requirements, as well as guidances disseminated by HHS after publication of the final rule. As documented head of the HIPAA task force, this officer oversees all the aspects of HIPAA implementation, ensuring timely adherence to the goals established by the members.

Although the school may maintain satellite clinics, only one privacy officer is required for the entire school system. This position does not need to be the only job of the appointed person, but the designated person should have time allocated to perform this extensive task.

HIPAA stipulates that the privacy officer of one covered entity can serve as the privacy officer of another covered entity, “so long as all the requirements of this rule are met for each such covered entity.” This means the privacy officer of a university-affiliated hospital or another professional school could be the privacy officer of the dental school. The scope of requirements that must be tailored to each of the multiple institutions, however, would in most likelihood extend beyond the capabilities of a single person.

The privacy officer can also assume the responsibilities of any other position on the committee. For example, he or she can be the security officer or the contact person. As head of the HIPAA task force, the privacy officer reports directly to the dean.

The selectee needs to be highly organized, willing and able to invest time in the project, and cognizant of the school’s clinical and administrative operations.
Contact Person

The contact person’s purpose is to receive complaints about privacy violations and to document the disposition of such complaints. He or she also provides information to patients about matters covered by the school’s privacy notice. The privacy rule has determined that “an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual’s rights and the covered entity’s legal duties with respect to protected health information.” The content of this notice can be found in the rule. The contact person must be mentioned in this notice at least by title. A possible candidate for this position is someone currently serving as a patient care advocate.

Security Officer

The security rule tasks a covered entity to “assess potential risks and vulnerabilities to the individual health data in its possession and develop, implement, and maintain appropriate security measures. These measures must be documented and kept current, and must include, at a minimum,” certain administrative, physical, and technical requirements and implementation features that are indicated within the rule.

While the rule does not specifically require a security officer, someone with at least a basic understanding of information systems and security mechanisms, as well as literacy in the formulation of policies and procedures, is needed to manage the rule’s security conditions. For the sake of objectivity, it is advisable that the security officer not be directly responsible for the school’s information system. An informatics person is a likely candidate or an administrative person with network level technical skills.

Training Officer

HIPAA stipulates the need for training all personnel who have contact with PHI to comply with the mandates, but does not specifically require a training officer. A school will need someone, however, to develop and implement a HIPAA training program. One potential candidate is the person responsible for Occupational Safety and Health Administration (OSHA) training and compliance.

Dean

An assistant/associate dean serves as a representative of the dean of the school. His or her presence ensures that this is a serious initiative that will move forward in a cohesive and timely fashion.

Sanctions Officer

According to the privacy rule, the dental school “must have and apply appropriate sanctions against members of its workforce” who fail to comply with the privacy policies and procedures of the dental school or the requirements found within the rule. Sanctions should be appropriate for the nature of a violation, ranging from a reprimand to termination. Policies and procedures for the application of appropriate sanctions must be developed and documented.

Civil and criminal penalties are possible for the misuse or misappropriation of health information. “Employees, agents, and contractors must be made aware that violations may result in notification to law enforcement officials and regulatory, accreditation, and licensure organizations.”

The sanctions official works with the contact person as well as the security and privacy officers to manage any violations. Reports should be generated to monitor infractions.

Representatives

Representatives of the school’s academic and staff departments should be willing to assimilate HIPAA requirements, clearly communicate the mandated conditions to associated personnel, and enlist the cooperation of all necessary personnel.

The Second Stage: Know What Is Required

All members of the HIPAA task force should begin to familiarize themselves with the HIPAA rules. A guidance for the privacy rule was posted July 6, 2001, that elucidated certain sections, such as minimum necessary disclosure, oral communications, and patient consent. Future modifications of the rules are expected.
The regulations should be read in their entirety and not in “bits and pieces.” It would be helpful for the privacy officer or another person to initially reformat the regulations into a usable and searchable document. Once the law is in a readable format, it can be disseminated to all task force members.

The regulations may be organized into a table listing all the requirements in one column, a column for current status of compliance with each requirement, and a final column for actions to be taken. This will serve as the basis for a gap analysis that indicates the difference between what is currently in place and what needs to be implemented for HIPAA compliance. A gap analysis provides the foundation for the risk analysis discussed later in this paper.

**Determine the Current State of Confidentiality**

The privacy rule emphasizes that administrative, technical, and physical safeguards must be in place to protect the privacy of protected health information (PHI) by the deadline. PHI encompasses all individually identifiable health information in electronic, paper, or oral form that is used or disclosed by the dental school. Part 1164 of the final privacy rule provides the “standards, requirements, and implementation requirements” that must be addressed in the gap analysis.

Before it can be protected, however, PHI should be identified in its multitude of forms and functions. The school should discover what information it has that is protected under the privacy rule and find out where it is stored and how and where it is transmitted. This action is necessary to provide school-specific applications for the requirements/implementation features contained within both the gap and risk analyses.

PHI identification is a time-intensive segment of HIPAA implementation. The passage of PHI should be mapped as it travels inside and outside the school. Members of the HIPAA task force can enlist staff and students to pursue the information flow. Flow charts are one means of organizing the movement, handling, and storage of information.

As PHI is mapped, questions concerning the security of each information item will be produced (see Table 1). Instances when current security policies and procedures may be inadequate should be indicated for correction.

Media for transmission may include fax, telephone, electronic, face-to-face encounters, and paper. Information may be in the form of a total record or a partial record.

It should be recognized that many areas/individuals come in contact with PHI: the chart room, scheduling, reception, surgery (periodontal and oral), insurance, research, dental hygiene students, student education, informatics, predoctoral and postdoctoral students, dental assistants, faculty, and information technology services (ITS).

In addition to people within the school, “business associates” who are not members of the workforce but to whom the school discloses PHI must be identified. Examples of business associates are attorneys and collection agencies.

The business associate requirements do not apply to those outside providers with whom the school shares PHI for treatment purposes. Business associate contracts or other arrangements are required when the school discloses information to someone or some organization that will use the information on behalf of the school or when the other person/organization will be creating or obtaining PHI on behalf of the school. Contracts are also needed when the business associate is providing specified services to the school and the provision of those services involves the disclosure of PHI by the school to the business associate.

After examining the result of information tracking, the task force has a picture of how well PHI is or is not protected within the school. The members should then compile a summary report of their findings.

During this period of time, the privacy officer is evaluating the current school policies and procedures. Some of these policies and procedures may already be HIPAA-compliant and are common practice, while others may be either not utilized or well documented. It is the privacy officer’s task to add this information to the previously mentioned gap analysis table. The gap analysis at this point will indicate privacy policies/procedures currently implemented and a listing of all those required under the privacy rule.

**Determine the Current State of Security**

A simple definition for security is those measures necessary to protect the privacy of an individual’s PHI. Loss of privacy can occur as a result of unauthorized disclosure or modification of PHI, destruction, loss and/or interruption of the services protecting PHI.
At the time of this article, the final rule for security had not been posted. The proposed security rule only addresses the protection of electronic transmission and information generated from these transmissions. The final privacy rule, however, encompasses written, oral, and electronic communication.

As with privacy, a gap analysis is necessary to determine the current and required states of security. Questions posed by Alberts et al.8 to use in a risk assessment are applicable to determining the current state of information security:

- What are the important information assets?
- What are the threats to these assets?
- What are the security requirements of the assets with respect to confidentiality, integrity, and availability?
- What is the organization currently doing to protect its information assets (current protection strategy)?
- What are the weaknesses in organizational policies and practice (organizational vulnerabilities)?

Evaluation of a school’s current state of security may be assisted by software that is available to assess a network’s vulnerability to intrusion.

This part of the initiative may seem to be the bailiwick of the software vendor or information technology services (ITS), but many of the requirements are administrative and not technical in nature. Additionally, what a vendor or ITS considers HIPAA-compliant may not address all the requirements. The security officer is the overseer of the security evaluation, ensuring that the technical and administrative requirements of HIPAA are met and documented.

Adequate security practices may already be in place, but lack supportive formal documented policies. The proposed security standards provide the requirements with implementation features that must be included in their operations. These requirements are loosely categorized under the headings of administrative procedures, physical safeguards, technical security services, and technical security mechanisms.9

The implementation features cover specific aspects of the requirements. In some instances, the feature is a stand-alone requirement, while in other instances a choice of features is presented.

Although the gap analysis will expose discrepancies, no technical changes should be initiated until after the risk analysis (explained in Stage Three). Technology and scope of implementation will be determined by the needs of the school.

### Pave the Way for Electronic Transactions Standards

Standards utilizing Electronic Data Interchange (EDI) were developed for the efficient and effective electronic exchange of health care financial and administrative transactions. ASC X12N standards to be utilized under HIPAA allow all covered entities to use one format for all of the following:

1. Health claims and equivalent encounter information.
2. Enrollment and disenrollment in a health plan.
3. Eligibility for a health plan.
4. Health care payment and remittance advice.
5. Health plan premium payments.
6. Health claim status.
7. Referral certification and authorization.
8. Coordination of benefits.

---

**Table 1. A sample of possible security questions used when mapping protected health information**

<table>
<thead>
<tr>
<th>PAPER</th>
<th>ELECTRONIC</th>
<th>ORAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>At what sites is the chart stored?</td>
<td>Where are the computer terminals?</td>
<td>Where are conversations held?</td>
</tr>
<tr>
<td>How is the storage area secured?</td>
<td>How are the terminals secured?</td>
<td>How secure are conversation areas?</td>
</tr>
<tr>
<td>Who accesses the chart at each location?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Is s/he authorized to read it?</td>
<td>• Is s/he authorized to read it?</td>
<td>Are only authorized personnel involved in the conversation?</td>
</tr>
<tr>
<td>• Is s/he authorized to modify it?</td>
<td>• Is s/he authorized to modify it?</td>
<td></td>
</tr>
<tr>
<td>• Does s/he clearly sign/date access?</td>
<td>• Who determines authorized access?</td>
<td></td>
</tr>
<tr>
<td>• Who determines authorized access?</td>
<td>• What security features are used for regulating access?</td>
<td></td>
</tr>
<tr>
<td>By what media does information leave the chart while in storage?</td>
<td>What media is used for transmission?</td>
<td>By what media does information leave the conversation area?</td>
</tr>
<tr>
<td>• What safeguards are used?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>By what media does the chart leave storage?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How, when, and by whom is PHI destroyed?</td>
<td>How, when, and by whom is PHI destroyed?</td>
<td></td>
</tr>
<tr>
<td>How are data aggregated for research, quality assurance, and surveys?</td>
<td>How are data aggregated for research, quality assurance, and surveys?</td>
<td></td>
</tr>
</tbody>
</table>
The implementation guides for the standards may be obtained from the Washington Publishing Company, 806 W. Diamond Ave., Suite 400, Gaithersburg, MD 20878; 301-949-9740 phone; 301-949-9742 fax. Guides may also be downloaded at no cost from www.wpc-edi.com/hipaa/.

In addition to the preceding standards, the rule only allows certain codes. Most dental procedures utilize CDT-3. In certain circumstances, however, dentists may need to rely upon CPT-4 (Current Procedural Terminology, 4th ed.), ICD-9-CM (International Classification of Diseases, 9th ed., Clinical Modification), HCPCS (Health Care Financing Administration Common Procedure Coding System), and UB 92.

According to Newton,6 each school should evaluate the application systems that send transactions and those that receive them. This includes examining both the types of transactions processed within the application system and the methods of transmission (example, TCP/IP), as well as describing the data sent. The application system owner and contact information should be identified along with local support for the system.

As the transition to HIPAA standards occurs, the system should be tested to ensure it is sending and receiving compliant transactions. Transaction certification is an option to test for compliance.

While the software vendors and ITS will provide the most assistance in achieving compliance for this rule, someone should be ultimately responsible for constructing the electronic transactions gap analysis and implementing the standards. The security officer is the best possible candidate.

As the deadline for this rule is October 16, 2002, standardization of electronic transactions should be an implementation priority unless an extension has been granted.

**Compose the Final Gap Analysis**

The privacy, security, and electronic transactions gap analyses are merged. The task force can make recommendations for actions that will close or narrow the gaps. Results are then compiled into a summary report that includes recommendations and implementation priorities.

**The Third Stage: Formulate a Risk Analysis**

After receiving the final gap analysis, the school’s administrative leadership works with the task force to perform a risk analysis. HIPAA defines risk analysis in the proposed security rule as “a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.”

When the law was drafted, no organization was expected to be able to fulfill all of the requirements to a maximum extent. Few health care organizations have the human, financial, or time resources to attain total compliance. For this reason, HIPAA has left the degree of compliance to the decision-making body of each covered entity. HIPAA is considered technology neutral because the law does not tell a dental school that one security measure is better than another.

Each dental school chooses how it wishes to implement the requirements established by HIPAA. Cost of implementation is generally the key factor in determining the degree of compliance.5 This is counterbalanced by the negative consequences6 that would occur if the measure were not implemented. These consequences, or losses, can be weighed in terms of risk. High risk means, for example, that the possibility of negative consequences is high if a chart is left in the waiting room.

Risk analysis is the “heart of compliance” because “this is the process by which an organization determines how much risk it will accept.”4 Once the school determines what it will accept as a result of the analysis, it can develop the administrative and technical policies to reduce the gaps discovered in the gap analysis and also determine the cost of implementation of the HIPAA initiative.

The following is a sample matrix used to explain possibilities of risk vs. cost of implementation.

<table>
<thead>
<tr>
<th>Risk (possibility of negative consequences if not implemented)</th>
<th>Cost of Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Computer passwords</td>
<td>Low</td>
</tr>
<tr>
<td>Low Storing a chart in a drawer or cabinet when not in use</td>
<td>High</td>
</tr>
<tr>
<td>Video cameras to monitor the clinic floor</td>
<td></td>
</tr>
</tbody>
</table>

The matrix deals with preventing unauthorized access to PHI. A requirement and its multiple applications must be carefully examined to determine what
cost the school is willing to pay and the amount of risk the school is willing to assume for noncompliance. For example, computer passwords are an easy, inexpensive method of blocking an intruder from accessing electronic patient information. Without passwords, the possibility of an unauthorized person accessing patient information in an open computer is high. A school could easily accept passwords but choose not to accept the high-cost alternative of restructuring the school to isolate all computers in locked rooms off the clinic.

A low-cost/low-risk example concerns the storage of a patient chart in an operatory of an open clinic during clinic hours. What is the chance an unauthorized person will read a chart if it is left on the operatory’s countertop? Even if the student and patient leave the operatory momentarily, a school may decide that the chance of an unauthorized person reading a chart left on the counter is low, that is, the possibility of negative consequences is low. The correct compliance action could then be the low cost establishment of a policy stating that unattended charts must be placed in drawers or cupboards. Another school may choose the higher cost option of enforcement using video cameras to ensure that unauthorized persons do not read the charts.

Once risk/cost has been evaluated, the requirements need to be prioritized within the categories of High Cost/High Risk, High Cost/Low Risk, Low Cost/Low Risk, and Low Cost/High Risk. Because medium risk and medium cost appear to be rare occurrences, this author chose not to include them in the chart.

Risk management follows the risk analysis, as the task force devises strategies to reduce risk to an acceptable level and maintain it at that level. HIPAA emphasizes that privacy/security solutions are reasonable: they do not need to guarantee safety. New security practices may be implemented, certain actions may be needed to maintain existing security practices, and identified vulnerabilities may need to be corrected. These strategies can be categorized by theme with an assigned person responsible for each theme. The various strategies are then presented in order of implementation. Funding, facilities, technology, and personnel are critical to this order.

The dean should review the final compliance plan before it is documented and executed.

The Fourth Stage: Implement Changes

The length of time for implementation will vary according to the complexity of the tasks. Many times, deadlines will need to be changed due to availability of technology and other deliverables. ITS may appoint a project manager whose primary responsibility is to serve as the liaison between the vendor and the dental school. The security officer works with vendors and/or ITS to achieve technical compliance within the designated timelines.

Policies and Procedures

A policies/procedures committee headed by the privacy officer begins the task of developing and documenting policies and procedures. The security officer also serves on this committee to handle the security administrative aspect.

A process should be in place so that policies and procedures can be created seamlessly during the transition. As policies are developed, procedures must be created to ensure that policies are followed.

A mechanism is necessary for policies/procedures to be reviewed with school personnel. This can be done at staff meetings or through the creation of memorandums or newsletters.

Policies and procedures, which can be stored in a readily available book or electronically, should be maintained, updated, and reviewed with staff as appropriate. In the event there is a compliance complaint against the school, it may not constitute a violation of HIPAA security requirements if reasonable, justifiable policies have been documented.

Legal Input

Legal representation works with the privacy officer to produce the required documents. Privacy needs include, but are not limited to, an individual consent form for the use/disclosure of PHI for treatment, payment, and operations (although this may change with the March 27 proposed modifications to the privacy rule); notice of information practices; individual authorization forms for use or disclosure of PHI; and business associate contracts/agreements. The attorney’s advice should be elicited for all policies and procedures.
Training

Training, which plays a major role in managing HIPAA implementation, must encompass all policies and procedures involving PHI that are required for the school’s workforce to carry out their functions.2 Management of oral, written, and electronic communications is included in this training.

As explained by Hjort,11 the training officer responsible for the development, documentation, and delivery of the training material could incorporate the following five components into the programs: awareness training; periodic security reminders; virus protection education; monitoring login success/failure and discrepancy reporting; and password management. Awareness training covers policies, procedures, and the importance of adherence. Periodic reminders in the form of newsletters, emails, and reminders at department meetings update what was learned through awareness training. Virus protection education instructs personnel on the etiology and effects of viruses on a health care system. Login success/failure and discrepancy reporting helps employees detect deviation from normal access patterns. Password management covers such topics as constructing an effective password, the need for not sharing passwords, and the importance of logging out when exiting the work area.

Each current member of the workforce must be trained by the compliance date. Those who are hired after the compliance date must be trained within “a reasonable period of time.”2

The Fifth Stage: Maintain the Implementation

HIPAA is an ongoing process that does not vanish with the implementation phase. Business strategies, budgets, hardware and software, and security technology will change over time. As previously mentioned, even the HIPAA rules can be modified on an annual basis.

The maintenance phase committee, composed of the contact person and the officers for privacy, security, sanctions, and training, are those who will ensure that any adaptations or innovations comply with the regulations. All modifications need to be supported by documented policies and procedures. The committee also needs to periodically evaluate the response to the implemented measures, identifying and handling any resulting concerns and/or issues. An additional task is updating the risk analysis on a regularly scheduled basis.3

Under the leadership of the privacy and security officers, a compliance plan and security management program should be operated on a continuing basis.3 A possible security strategy includes auditing security practices annually; reauditing if any incident occurs when a procedure is not followed; and documenting everything.4 The privacy officer should be on the alert for breaches in policy/procedure/practices, managing any incidents reported by the contact person. The privacy and security officers should provide the dean with regular reports.

Training is ongoing. Whenever a change occurs in technology, policies, and/or procedures as a result of either the school’s or HIPAA’s actions, staff whose functions are affected must be trained again within a reasonable period of time.

The staff learning curve will be steep, as the school adapts to the cultural change. Resistance in the form of lack of compliance is expected; change is difficult for busy health care personnel. This type of reaction was encountered during the OSHA initiative. To overcome this, appropriate sanctions need to be enforced, and the administration’s continued visible advocacy is imperative.

Conclusion

HIPAA is not just an information technology initiative. There are legal, regulatory, operational, and security issues that must be juggled along with technology to achieve compliance by the designated deadlines. Unlike the Y2K initiative, the compliance process will not end on the striking of a clock; it must become woven into the culture and technology of each covered entity.

This paper proposes one possible HIPAA strategy for compliance that can provide the guidance needed by dental schools. No two schools will have the same strategy. Each dental school needs to adapt the implementation to its own unique organizational structure as there is no “one size fits all” strategy.

There is also no quick fix to meet HIPAA requirements. The entire compliance process demands a significant investment of time and resources. Precise assessment of costs (and benefits) is difficult when there is no historical experience with HIPAA. While the costs may be significant in the beginning,
the preamble to the privacy rule explains the rationale behind the government’s belief that the return on investment from administrative simplification will be positive.

Although the task appears formidable, HIPAA compliance is not an impossible quest. Requirements may seem too onerous for implementation, but an organizationally appropriate plan of action, coupled with cognizance of policies/procedures already instituted within a school, enables a HIPAA task force to approach this challenge in a logical, step-by-step manner. The initiative can be seen as an opportunity for dental schools to retool their practices and demonstrate to the public a commitment to improving the quality of health care, while protecting the privacy rights of patients.

REFERENCES