

# Chapter 12

## Physician as an Employer

Charles G. Hess, MS, MD

Hazard Communication Standard  
Americans with Disabilities Act  
Blood-Borne Pathogens Standard

Clinical Laboratory Improvement Amendments  
Health Insurance Portability and Accountability Act

Federal laws passed in the United States since 1980 have profoundly affected the practice of medicine. The government's control over the practice of medicine reached new heights with the passage of the Health Insurance Portability and Accountability Act (HIPAA) in 1996. When the Department of Health and Human Services (DHHS) made the standard effective on April 14, 2001, medicine entered the electronic age. The purpose of this chapter is to outline the physician's legal responsibilities, in his or her role as a physician-employer, in some of the more important regulations.

### HAZARD COMMUNICATION STANDARD

Some of the almost 600,000 chemical products in the United States pose serious problems for exposed employees.<sup>1</sup> In 1983, the Occupational Safety and Health Administration (OSHA) issued a regulation called *hazard communication* that applied to employers in the manufacturing sector. Under the Hazard Communication Standard (HCS), the employee is required to be informed of the contents of the law, the hazardous properties of chemicals encountered in the workplace, and measures (such as safe handling procedures) needed to protect employees from these chemicals. The law was expanded in 1988 to include employers in the non-manufacturing sector such as the physician-employer; thus HCS became the first regulation to concern itself specifically with the health and safety of medical employees.<sup>2</sup>

Under the general duty clause of this law, the physician-employer "shall furnish a place of employment which is free from recognized hazards that are causing or are likely to cause death or serious physical harm to his or her employees." The physician is required to post the Job Safety and Health Protection Poster (OSHA Form 2203) in the office or clinic. Forms that have been updated are Forms 300 (Log of Work-Related Injuries and Illnesses), 301 (Injury and Illness Incident Report) and 300A (Summary of Work-Related Injuries and Illnesses). Since January 2003, work-related hearing losses and musculoskeletal disorders have had to be reported.

#### Hazard Communication Plan

Under HCS, every physician-employer who has one or more employees exposed to a hazard is required to develop

a written program to protect those individuals. The hazard communication plan (HCP) must outline those health and safety policies and procedures placed into effect by the employer to protect his or her workers.

#### Hazardous Chemicals

A complete inventory must be taken once a year of all products in the office or clinic. The HCS requires that all chemicals imported, produced, or used in a workplace undergo a "hazard determination." This evaluation, which may be delegated to an employee, should include not only medical supplies (such as isopropyl alcohol and bleach), but also office supplies (such as correction fluid and copier toner).<sup>3</sup> OSHA considers products to be hazardous when a hazardous chemical makes up 1% or more of the product or a carcinogen makes up 0.1% or more of the product. There are essentially two ways to determine whether a product is considered hazardous. One way involves asking the product's manufacturer or distributor for a material safety data sheet (MSDS); the other involves comparing chemicals in office products with those on lists prepared or recommended by OSHA.

Most consumer products containing hazardous chemicals that are used in the office are cleansing agents.<sup>4</sup> Medications that are dispensed by a pharmacist to a physician for direct administration to a patient are exempt.<sup>5</sup> Drugs in solid form (pills or tablets) are also considered exempt, as well as most injectables and other medications used in the office settings.

#### Material Safety Data Sheets (MSDS)

A material safety data sheet is an informational sheet furnished by a product's manufacturer to the user in order to identify the hazardous characteristics of the product. Every hazardous product must have a MSDS, provided by the manufacturer or distributor on written request. In 1986, OSHA developed Form 174 to provide a universal form that would meet the HCS requirements; use of the form is not mandatory, but OSHA requires all the information on the form.

Once a year, requests should be made for MSDSs on all hazardous products that have been changed or are new to the office. Such sheets should be kept for 5 years.<sup>6</sup> MSDSs may be kept on electronic equipment provided that "there are no barriers to employee access."<sup>7</sup> Under the present rule,

## 116 Physician as an Employer

drug package inserts cannot be accepted in lieu of MSDSs for “less than solid” drugs (creams, ointments, liquids, and injectables).<sup>8</sup> Drug samples, if not used in the office, do not require MSDSs.

### Hazard Labels

After MSDSs are obtained, if not “rated,” they have to be rated in order to create hazard labels. Under HCS, the practice is required to label, tag, or mark hazardous chemicals in the office or clinic. The purpose of the label is to serve as an “immediate warning” and as a “reminder of more detailed information” in the MSDS. Instead of labeling specific containers, OSHA permits the posting of proper information on the front or back sides of cabinet doors where hazardous materials are stored.<sup>9</sup> The label must show the identity of its hazardous chemical or chemicals and any appropriate hazard warnings. There is no single labeling system recommended by OSHA. The most widely used label is an adaptation of one developed by the National Fire Protection Agency (NFPA 704 Standard). The NFPA label is a diamond-shaped, color-coded label, with a different color for each represented hazard.

### Training Program

HCS requires employers to provide a training program for all employees exposed to hazards in the routine performance of their duties. As with training programs under other standards, employees must be trained at scheduled staff meetings, with each session documented on a training log.

## AMERICANS WITH DISABILITIES ACT

In 1990 the Americans with Disabilities Act (ADA) was passed to prevent unfair discrimination against disabled persons with visual, hearing, and other physical and mental impairments. This law prohibits discrimination on the basis of disability and protects qualified applicants, employees, and the general public who have disabilities from discrimination in all aspects of employment and public access to services and facilities.<sup>10</sup> All sorts of disabilities are covered, including persons with cancer, human immunodeficiency syndrome (HIV), blindness, deafness, attention deficit disorder (ADD), learning disabilities, mental retardation, and mental illness. Individuals who are former drug or alcohol abusers are also covered under ADA. The law requires the physician to place a poster in his or her office describing the provisions of ADA.

As a five-part regulation, ADA requires several different aspects of compliance. Only Titles I and III, however, are applicable to medical practices.

### Title I

The original law prohibited job discrimination in offices with 25 or more employees after July 26, 1992. The present law, however, exempts only those employers with fewer than 15 employees. Under Title I, the employer must use the same employment standards in all hiring, paying,

training, promoting, and firing decisions. Neither the physician-employer nor any of his or her office staff may engage in any illegal job-recruiting or job-interviewing practices. For example, during a job interview, the employer cannot inquire about a history of disability, illness, absenteeism, or workers' compensation benefits. The employer cannot ask the applicant about the presence of a disability but can ask about the applicant's ability to perform certain tasks. Also, a physical examination cannot be performed until an offer of employment has been made. Although the applicant can be excluded for his or her inability to perform “essential” tasks, the applicant cannot be excluded for an inability to perform “marginal” tasks. If a disabled person applying for a job is judged to be the best-qualified applicant (without consideration of the applicant's disability), ADA requires the employer to hire that individual. Also, a physician-employer cannot decide against hiring a disabled person because employment of that individual would require “reasonable accommodation,” that is, “one that does not cause significant difficulty or expense in relation to the employer's operations, financial resources or facilities.”<sup>11</sup> Additional stipulations in this section require employers to make certain accommodations for disabled persons already employed.

### Title III

Under Title III, the physician is responsible for making his or her practice accessible to persons with disabilities. As of January 26, 1992, persons owning, leasing, or operating places of public accommodation must reasonably alter their policies, procedures, and practices to promote equal opportunities for all individuals.<sup>12</sup> All existing health care facilities must make their common use areas “accessible” if removal of structural barriers is “readily achievable,” that is, “easily accomplished and able to be executed without much difficulty or expense.”<sup>13</sup>

### Access

Accessibility guidelines for new construction and alteration of the existing structures have been developed for ADA. For example, an adequate number of “accessible” parking spaces should be provided—at least one accessible space for every 25 parking spaces. Furthermore, one of every eight accessible parking spaces must be van-accessible and so marked.<sup>14</sup> Total compliance is required only for new construction and alterations. Tax incentives are available for the removal of architectural barriers.

### Auxiliary Services

The ADA requires the physician to provide (and pay) for those auxiliary aids and services necessary to ensure effective communication with individuals “unless an undue burden or fundamental alteration of services would result.”<sup>15</sup> In some cases, office policies and procedures may have to be altered. For example, an office or clinic may need to allow the entry of guide dogs for blind patients. With

regard to auxiliary aids, the needs of the patient must be considered in deciding whether to use a notepad, Brailled materials, other formats (e.g., audiotape), or an interpreter.

Does the physician have to hire a sign-language interpreter? The area of concern to most physicians is how to deal with hearing-impaired patients. The answer to the question is “maybe.” Although the intent of the law is to require appropriate auxiliary aids and services “when necessary,” the service must not cause “significant difficulty or expense.”<sup>16</sup> The law does not impose on a physician the requirement that primary consideration be given to a disabled person’s requests. In most cases, an interpreter should not be needed if a patient can read questions and write answers. Another alternative to the use of a notepad is a computer terminal on which the physician and patient can exchange typewritten messages. The Justice Department cites situations in which it believes the services of an interpreter are needed.<sup>17</sup> One example is when a hearing-impaired person needs to undergo major surgery; other areas besides health include financial, legal, and personal matters. The end result, however, is that “in those situations requiring an interpreter, the public accommodation (such as a physician’s office or clinic) must secure the services of a qualified interpreter, unless an undue burden would result.”<sup>18</sup>

## BLOOD-BORNE PATHOGENS STANDARD

The second federal law to concern itself with the safety of medical employees was the Blood-Borne Pathogens Standard (BBP) of 1991, by OSHA. The intent of this law is to reduce exposure in the health care workplace to all blood-borne pathogens, particularly the hepatitis B virus (HBV) and HIV. Hepatitis B virus infection is considered the major infectious blood-borne occupational hazard to healthcare workers. In 2003, the Center for Disease Control and Prevention (CDC) reported the estimated number of new cases of HBV at 73,000 (and of Hepatitis C virus [HCV] at 30,000).<sup>19</sup> Of adults reported with AIDS in the United States through December 31, 2002, 24,844 had a history of employment in health care; as of November 2005, 57 health care workers have seroconverted to HIV following occupational exposure.<sup>20</sup>

### Exposure Control Plan

Any employer having at least one employee with occupational exposure is required to have a written exposure control plan (ECP). The stated purpose of the plan is to eliminate or minimize occupational exposure to blood and other potentially infectious materials. The employer is required to make a copy of this plan available to all employees and any OSHA representative. It must be reviewed and updated at least once a year.

### Exposure Determination

Each employer who has one or more employees with occupational exposure is required to perform an exposure

determination. The exposure determination list consists of the following:

1. A list of job titles in which all employees have occupational exposure;
2. A list of job titles in which some employees have occupational exposure; and
3. A list of all tasks (or groups of closely related tasks and procedures) that identify certain employees within a job classification where some, but not all, employees have occupational exposure

### Exposure Incident

The ECP must also explain how the employer will evaluate the circumstances surrounding exposure incidents. This evaluation should include the circumstances of the incident, synopsis of present controls, and evaluation of present “failures.” Additionally, medical practices with more than 10 employees are now required to keep a log that describes all sharps-related injuries, detailing how, when, and where injuries occurred and what device was involved.

### Exposure Control

BBP law was drafted so that employees will be protected by performance-oriented standards. The specific provisions of the ECP are an effort to make clear “what is necessary” to protect employees. It is the responsibility of the physician-employer to limit worker exposure through implementation of the following categories of control: universal precautions; workplace controls; personal protective equipment; housekeeping policies; hazard communication policies; a hepatitis B program; and a training program.

#### Universal Precautions

OSHA’s method for reducing exposure to blood-borne pathogens is based on the adoption of universal precautions as the foundation for a plan of infection control. Under BBP, workers are required to exercise universal precautions to prevent contact with blood or other potentially infectious materials.

#### Workplace Controls

Workplace controls are of two types: engineering controls and work practice controls. Engineering controls reduce employee exposure by either removing the worker from the hazard or removing the hazard itself. Examples of engineering controls are sharps containers, biosafety cabinets, and self-sheathing needles. Work practice controls reduce employee exposure by altering the manner in which a procedure is performed. The employer is required to incorporate the following work practice controls into the ECP: washing hands, and handling blood, equipment, personal items, and sharps. Employees must not bend, break, or shear contaminated needles and other contaminated sharps. Contaminated needles and other contaminated sharps cannot be recapped or removed unless it can be demonstrated that no alternative is feasible or that such action is required by a specific medical procedure.

## 118 Physician as an Employer

With the passage of the Needlestick Safety and Prevention Act, which became effective in April 2001, medical practices have to consider safer needle devices as part of the reevaluation of appropriate engineering controls during the annual review of the ECP. The physician-employer, together with frontline employees who actually handle the sharps, must choose, evaluate, and implement such safety-engineered devices.<sup>21</sup> Such "good faith" efforts to determine if any of the newer devices is applicable to the practice must be documented.

### Personal Protective Equipment

When engineering and work practice controls are insufficient to eliminate exposure, personal protective equipment (PPE) must be used "to prevent or minimize the entry of materials into the worker's body."<sup>22</sup> BBP states that "when there is occupational exposure, the employer shall provide, at no cost to the employee, appropriate personal protective equipment such as, but not limited to, gloves, gowns, lab coats, face shields or masks and eye protection, and mouthpieces, resuscitation bags, pocket masks, or other ventilation devices." OSHA places the responsibility of protecting employees directly on the employer. The employer must not only provide appropriate PPE, but also make sure that it is used "when necessary."

### Housekeeping Policies

BBP requires employers to keep workplaces "in a clean and sanitary condition." Under housekeeping policies, the employer is required to schedule, and then to implement, a written agenda for cleaning and decontaminating the office, including the following: cleaning of surfaces, equipment, and linens, and discarding of regulated waste.

### Hazard Communication Policies

BBP requires the use of hazard communication through labels or signs to ensure that employees receive adequate warning in order to eliminate or minimize their exposure to blood-borne pathogens. Such labels are to be affixed to refrigerators and freezers containing blood or other potentially infectious material, as well as other containers used to store, transport, or ship blood or other potentially infectious materials. Red bags or red containers may be substituted for labels.

### Hepatitis B Program

The employer is required to make the hepatitis B vaccine available to all employees who have occupational exposure. Ordinarily, the hepatitis B vaccination series has to be offered within 10 working days of the initial assignment at no cost to the employee. Those who decline to accept the vaccination must sign a statement to that effect. For those who have had an exposure incident, the employer is also required to obtain a postexposure evaluation and a medical follow-up examination. After an exposure incident, the employer is required to provide the employee with the following information:

1. The route and circumstances of exposure;
2. The name of the source individual (unless impossible); and
3. The results of the source individual's blood test, if available.

The employer is required to furnish the employee with a copy of the evaluating physician's written opinion within 15 days of receipt of his or her report. As part of the medical follow-up examination, the employee is entitled to prophylactic medications (if recommended by the U.S. Public Health Service), counseling sessions, and medical evaluation of postexposure illnesses. Medical records for each employee with regard to hepatitis B vaccination and occupational exposure must be kept for the duration of the employment plus 30 years.

### Training Program

Training about the hazards associated with blood and other potentially infectious materials must be provided by the employer to all employees with occupational exposure. The employer is required to keep training records for all employees with occupational exposure for 3 years from the date on which the training occurred. The same rules that apply to medical records also apply to training records.

## CLINICAL LABORATORY IMPROVEMENT AMENDMENTS

The 1988 Clinical Laboratory Improvement Amendments (CLIA) were passed to ensure the accuracy of laboratory tests performed on human specimens. Most of the regulations became effective on September 1, 1992. The physician is no longer able to perform tests on patients in his or her office without legal permission from the federal government.

### Certification

This law requires all laboratories, including physician office laboratories (POLs), to obtain one of five certificates: a registration certificate, a certificate of waiver, a certificate of provider-performed microscopy, a certificate of compliance, or a certificate of accreditation. Even if only one test is performed (and even if no charge is made for that test), the Health Care Financing Administration (HCFA) requires the physician-employer to obtain a certificate. Once an application is received, HCFA may issue a registration certificate, together with a CLIA number (for requests for laboratory testing reimbursement made to Medicare or Medicaid third-party payers after January 1, 1994).

A registration certificate permits a laboratory to continue operations for 2 years or until a determination of compliance can be made, whichever is shorter. The certificate of accreditation can be issued by the Commission of Office Laboratory Assessment (COLA) to those laboratories (including POLs) desiring an alternative to federal inspections under CLIA. Also, a laboratory in a state with a federally approved licensure program may choose to receive a state license in place of a CLIA certificate, provided it complies with the regulations of that state.

### Categories of Tests

Present laboratory tests, numbering about 10,000, have been classified according to the degree of difficulty in the

performance of the test.<sup>23</sup> This ranking initially resulted in a three-tier organizations of tests into categories called *waived*, *moderate complexity*, and *high complexity*, to which a fourth category (now called *provider-performed microscopy*) was added in February 1993. Depending on its certification, a laboratory can perform tests in one or all four categories.

A laboratory that limits itself to performing waived tests is essentially exempt (except for manufacturers' instructions) from CLIA requirements. Procedures classified under provider-performed microscopy must be performed by either the physician or a health care provider, in conjunction with an examination of the patient in the office. Laboratories performing waived and provider-performed microscopy tests are not subject to routine inspections, but are subject to random compliance and complaint investigations.

### Nonwaived Tests

Those laboratories performing provider-performed microscopy, moderate-complexity tests, and high-complexity tests must fulfill certain requirements for personnel standards, patient test management, quality control, proficiency testing, and quality assurance.

### Personnel Standards

Each laboratory performing nonwaived tests must meet certain personnel standards (PS), which are tied to the complexity of the testing process. The rules, which differ for moderate-complexity testing and high-complexity testing, list detailed personnel responsibilities and qualifications; qualifications are based on formal education, laboratory experience, and/or laboratory training. Laboratories performing tests in the moderate-complexity category must employ a laboratory director, technical consultant, clinical consultant, and testing personnel. Laboratories performing tests in the high-complexity category must employ a laboratory director, technical supervisor, clinical consultant, general supervisor, and testing personnel.

### Patient Test Management

Each laboratory performing nonwaived tests is required to have in place a system ensuring the correct performance of the entire testing process, beginning with the preparation of the patient and ending with the distribution of test results. Patient test management (PTM) consists of two parts: (1) written policies and (2) documentation (to verify the former).<sup>24</sup> The regulations require written policies for the following: preparing patients, processing (collecting, preparing, identifying, storing, transporting, and discarding) specimens, and reporting results.

With regard to test results, normal or reference ranges must be available, but they need not be printed on the reports. The laboratory is also required to develop a written policy (or protocol) to follow when a life-threatening or "panic" value occurs. The protocol demands that the individual ordering the test or the individual responsible for utilizing the test results be notified immediately when any test result indicates an immediate danger to a person's life.

With the second part of PTM, three documents are required: the test requisition, the test record (patient log), and the test report, all of which must be retained for a minimum of 2 years. Tests can be performed only on the oral, written, or electronic order of an "authorized" person. That authorized person will usually be the physician (or another state-authorized individual). The authorized person must sign written requests; oral orders are permitted as long as written orders are obtained within 30 days. The "three R's" of PTM allow a laboratory to track and positively identify patient specimens as they move through the complete testing process. Specific information must be contained in these three documents to comply with the law.

### Quality Control

Manufacturers of instruments, kits, and test systems usually provide guidelines for quality control (QC) of their products. One kind of internal QC procedure involves the use of QC samples; these samples, similar to patient specimens, have known test results. QC samples, when run at the same time as patient specimens, can provide the operator with a "within run" check to confirm test results.<sup>25</sup> Each laboratory performing nonwaived tests is required to develop and follow written QC procedures that monitor the quality of the analytic testing process of each test method. Of the two sections on QC, one contains general requirements, and the other contains special requirements for specialties or subspecialties.

Laboratories using uncleared tests must follow the full QC rules. Full QC rules are also required for all tests of moderate complexity that have been cleared but have been modified or developed in-house and for all tests of high complexity.

### Proficiency Testing

One way of making sure a particular laboratory's performance is in line with that of other laboratories performing the same analysis involves the testing of unknown samples from an outside source. Just as QC samples provide a type of internal QC, proficiency testing (PT) offers a kind of external QC. Each laboratory performing tests of moderate or high complexity must enroll in an approved PT program for all specialties or subspecialties in which it desires to be certified. The PT provider must be either a private, nonprofit organization or a federal or state entity.

Once the laboratory has been enrolled, the PT provider will send samples to its subscriber three times a year; each shipment includes five samples for that "event." The samples, whose values are not known, are run along with the laboratory's regular workload of patient specimens. It is unlawful to send portions of PT samples to other laboratories for "comparison" studies. The final results are sent to the PT provider, together with an attestation from signed by both the operator and the laboratory director. For most tests, the minimum passing score is 80%.<sup>26</sup> Any laboratory failing two consecutive or two out of three testing events will be subject to sanctions (including cancellation for that specialty, subspecialty, or test).

## 120 Physician as an Employer

### Quality Assurance

Every laboratory performing nonwaived tests must implement and follow written policies and procedures for a quality assurance (QA) program designed to monitor and evaluate the quality of the total testing process. CLIA is the first standard to require a QA program as part of the law. It is the responsibility of the employer, as laboratory director, to ensure the accuracy of test results and the adequacy of laboratory services. In a POL, laboratory testing may be done by two workers or one worker and the director; in such cases, all members should make up the QA committee. The QA committee is responsible for making sure that "quality" evaluations take place and that corrective actions take place whenever problems are identified; to reach this goal, the seven key elements to be addressed are:<sup>27</sup> (1) procedure manual; (2) personnel standards; (3) patient test management; (4) quality control; (5) proficiency testing; (6) complaint investigations; and (7) quality assurance review.

## HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The purpose of the 1996 Health Insurance Portability and Accountability Act (HIPAA) was to make health care insurance "portable," so that an individual's insurance could be passed from one employer to another employer. Because of additions to help fight fraud and abuse, ensure the security of medical records, protect the privacy of a patient's confidential health information, and a worthwhile goal to replace paper transactions with electronic transactions, the HIPAA Standard has become one of the most comprehensive and complicated regulations ever passed.<sup>28</sup> Under HIPAA, the physician-employer must make sure his employees conduct themselves in a manner that supports the provisions of this ambitious standard. Four of the categories that fall under the part of HIPAA known as the Administrative Simplification Act presently concern us: the Transactions and Code Set Rule, the Privacy Rule, the Security Rule, and the National Provider Identifier.

### Transactions and Code Sets Rule

#### Transactions Standards

If a medical office processes financial and administrative transactions electronically, either itself or through a vendor who transmits them to a health plan electronically (billing service or clearinghouse), that office falls under the Transactions Rule. This rule does not affect paper transactions. The intent of this piece of HIPAA was to replace the 437 different formats for online processing of health claims.<sup>29</sup> With a single standard claim form, replacing electronic versions of the HCFA 1500 and UB 92, the Department of Health and Human Services (DHHS) would be able to establish national standards for health care transactions and code sets. The original compliance deadline was October 16, 2002; however, a one-year extension

was granted to those practices filing the CMS Model Compliance Plan.

Each transaction standard has to have specific format and content requirements in order to be processed by health plans and clearinghouses. Originally, the Transactions Rule specified standards for the following transactions:<sup>30</sup>

ASC X12N 837	Health Claims or Encounter Information
ASC X12N 835	Payments and Remittances
ASC X12N 837	Coordination of Benefits (COB)
ASC X12N 276/277	Health Care Claim Status
ASC X12N 834	Enrollment and Disenrollment
ASC X12N 270/271	Eligibility Verifications
ASC X12N 820	Health Plan Premium Payments
ASC X12N 278	Precertifications and Referral Authorizations

### Code Sets

The Transactions Rule also requires the use of national code sets. Use of the current versions of the medical code sets ICD-9-CM, CPT-4, and HCPS is required. Local codes have been eliminated. Other standard code sets (such as zip codes) are also required.

### Options

To achieve compliance with the Transactions Rule, the physician-employer has several options:<sup>31</sup>

- Comply with both content and format requirements:  
Send the HIPAA-compliant transactions directly to health plans
- Comply with both content and format requirements:  
Send some HIPAA-compliant transactions directly to health plans  
Send other HIPAA-compliant transactions to clearinghouses
- Comply only with content requirements:  
Send nonstandard formats to a clearinghouse (to format) and the then HIPAA-compliant transactions to a health plan.
- Comply only with content requirements and use direct date entry (DDE) to send non standard formats to health plans accepting DDE.

### Transactions Officer

Before the medical practice begins the laborious task of software reprogramming, the physician needs to employ or appoint a "transactions officer." It is this individual who will help the physician bring the office into compliance. The transactions officer is responsible for inventorying present transactions, assembling vendor data, discovering data gaps, and finally ensuring the new computer system is HIPAA-compliant. His or her duties may be summarized as follows:

1. *Inventorying duties:* The transactions officer must prepare inventory lists, matching transactions with all vendors (their billing products), clearinghouses, and health plans.
2. *Data-assembling duties:* After completing the inventory lists, the transactions officer must communicate orally or in writing with the practice's vendors, clearinghouses, and health plans to discover their plans and timetables

for becoming compliant; relevant information should be recorded in the inventory lists.

3. *Data-discovering duties:* The upgraded system should allow for the “capturing” of new data elements required by the “837 Professional Claim.”
4. *Managing duties:* After assembling all the information concerning the practice’s vendors, clearinghouses, and health plans, the physician, with the help of the transactions officer, must make final decisions on specific strategies for compliance.

### Implementation

Ideally, the software should permit the office to conduct all the transaction types directly with health plans. At the least, the practice should be able to supply the content for transactions to a clearinghouse. The office will have to choose one of three possible solutions:<sup>32</sup>

- upgrade the present billing software;
- submit claims to a clearinghouse;
- purchase a new computer system with HIPAA-compliant billing software.

### Training Program

After the installation of upgraded or new software (and the entering of additional data elements), the transactions officer should begin training employees. Once the training has been completed, the practice’s vendor should be able to supply test data that will put the system through all possible transaction scenarios. Finally, employees should do computer-to-computer testing to ensure that the office’s computer system can transmit information from the office through any clearinghouse and on to any health plan.

### Privacy Rule

The Privacy Rule basically controls what is called protected health information (PHI). PHI is individually identifiable health information that is held or released by a practice regardless of how it is communicated (oral, paper, or electronic). The entire Privacy Rule was created to make sure that a patient’s PHI is not used or disclosed to those individuals or parties that do not need to know such information. This rule is discussed in Chapter 16.

### Security Rule

Whereas the Privacy Rule covers all forms of a patient’s PHI (oral, written, or electronic), the Security Rule applies only to protected health information that is electronic (E PHI), whether it is created, received, maintained, or transmitted. The rule does not cover PHI that is transmitted orally or stored on paper. Additionally, while the Privacy Rule is concerned with those granted access to PHI, the Security Rule is concerned those granted access *actually have* access to E PHI. E PHI can be transmitted over the Internet or stored on a computer, a CD, a disk, magnetic tape, or some other object (such as a PDA or cell phone).

Why is there a need for the Security Rule? One good answer is the possibility of malicious electronic attacks

### Health Insurance Portability and Accountability Act 121

(such as a hacker changing the HIV status of a patient or adding “high-risk information” to a patient’s record “for fun”) or an employee revealing or even selling a patient’s confidential medical information.<sup>33</sup> Under the Security Rule, physicians are required to assure the integrity (unaltered data), availability (disaster recovery), and confidentiality (authorized access) of an individual’s PHI that is electronically collected, used, transmitted, or stored. The compliance date for the Security Rule was April 20, 2005.

### Security Standards

The Security Rule requires practices to develop safeguards for collecting, using, transmitting, and storing PHI in a secure environment. Since there is a lot of overlap between the Privacy Rule and the Security Rule, some practices may have already fulfilled some of the requirements. In developing the standards for this rule, the DHHS followed closely the requirements of the Privacy Rule, with safeguards described as administrative, physical, and technical.<sup>34</sup>

### Implementation Specifications

The requirements of the Security Rule are far more comprehensive than those of the Privacy Rule, with a level of detail unmatched in previous rules. Of the 18 Security Standards concerning the physician-employer, there are 42 implementation specifications, with 20 described as “required” without further instructions (these are a “must”) and 22 described as “addressable” (with flexible options).<sup>35</sup>

In approaching the “addressable” specifications, the physician is urged to consider the size and complexity of his practice, his technical infrastructure (hardware, software, and security capabilities), cost, and probability and criticality of potential risks to E PHI.<sup>36</sup> Any time an employer decides that an “addressable” implementation is unreasonable, he must document the reasons why—and what has been done as an alternative. “The Standards do not allow organizations to make their own rules, only their own technology choices.”<sup>37</sup>

### Security Officer

The initial step in the endeavor to satisfy all the implementation specifications is the appointment of a security officer (or, in large clinics, a security committee). This individual will be responsible for developing, implementing, and monitoring the security policies of the office. It is his or her duty to report to the physician-employer the status of ongoing compliance efforts. Training and sanctioning duties are similar to those of the privacy officer.

### Implementation Steps

At least six steps are needed to bring a practice into compliance: HIPAA gap analysis, E PHI inventory,<sup>38</sup> risk analysis,<sup>39</sup> risk management,<sup>40</sup> an action plan (e.g., a check sum, double keying, a message authentication code, or digital signature),<sup>41</sup> and security policies and procedures to facilitate periodic evaluation.<sup>42</sup> Security policies and procedures must be kept for 6 years.

## 122 Physician as an Employer

### National Provider Identifier

Demonstrating that HIPAA is far from over, the National Plan and Provider Enumeration System (NPPES) announced that it would accept applications for National Provider Identifiers (NPIs) as of May 23, 2005. The goal of the NPI is to eventually replace all other identifiers that providers use to process electronic health care transactions. Practices will need to have a NPI, because it will ultimately be needed for all orders, prescriptions, and claims for payment.<sup>43</sup> Practices can apply online, by mail, or an entity may apply for the employer on his behalf. The compliance date is May 23, 2007.

### Endnotes

1. A. McLaughlin & J. Pendergrass, *Hazard Communication: A Compliance Kit A-1* (US. Government Printing Office, Washington, D.C. 1988).
2. L. Traverse, *The Generator's Guide to Hazardous Materials/Waste Management* 119 (Van Nostrand Reinhold, New York 1991).
3. Program notes, Eagle Associates seminar, presented by Joseph Suchocki (Apr. 1990).
4. J. Suchocki et al., *The Safety Resource Guide for OSHA Compliance*, 12 (Eagle Associates, Ann Arbor, Mich. 1990).
5. *Hazard Communication Changes*, Am. Prac. Adv. 115 (1994).
6. *The Illusive Material Safety Data Sheet*, Am. Prac. Adv. 120 (1993).
7. *Supra* note 5, at 17.
8. *Alert for Material Safety Data Sheets*, Am. Prac. Adv. 77 (1993).
9. *Questions and Answers*, Am. Prac. Adv. 10 (1992).
10. *The Americans with Disabilities Act of 1990*, Am. Prac. Adv. 43 (1995).
11. *Reviewing the Americans with Disabilities Act*, Am. Prac. Adv. 43 (1995).
12. *The Americans with Disabilities Act of 1990*, Am. Prac. Adv. 47 (1992).
13. *Id.*
14. *Supra* note 12, at 49.
15. *What Every Doctor Needs to Know (Americans with Disabilities Act)* [information sheet] (American Medical Association 1990).
16. H. Barton, *Physicians Discover Maze of Regulations under ADA*, 88(11) Tex. Med. 55 (1992).
17. *Id.* at 56.
18. *Id.*
19. CDC, *Summary of Notifiable Diseases, United States 2002*, MMWR 2003:51(63).
20. [www.cdc.gov/ncidod/hip/BLOOD/hivpersonnel.htm](http://www.cdc.gov/ncidod/hip/BLOOD/hivpersonnel.htm).
21. *Trainers Notes: Bloodborne Pathogens*, Am. Prac. Adv. 13 (2003).
22. Occupational Exposure to Bloodborne Pathogens (summary), 29 C.F.R. Part 1910.1030 at 64124.
23. *CLIA 1988 Compliance* [information sheet] 4 (American Proficiency Institute 1993).
24. *Patient Test Management System Trilogy*, Am. Prac. Adv. 61 (1992).
25. *Supra* note 24, at 9.
26. *Regulations for Implementing Clinical Laboratory Improvement Amendments of 1988: A Summary*, 267 J.A.M.A. 1731 (1992).
27. C. Hess, *Office Compliance Manual* 91 (All-Med Press, Houston 1995).
28. *HIPAA: Unraveling the Mystery for Medical and Dental Practices*, Am. Prac. Adv. 2 (2002).
29. Program notes, HIPAA Compliance Alert Seminar, presented by George Lilly (Nov. 20, 2002).
30. [www.hipaadvisory.com/action/archives/Trans-CodeSetsGuide.htm](http://www.hipaadvisory.com/action/archives/Trans-CodeSetsGuide.htm).
31. *Supra* note 29.
32. *Id.*
33. Program notes, Network Security and HIPAA Preparedness seminar, presented by S. Fontenot (Mar. 2005).
34. *Id.*
35. 68 Federal Register 8380, Feb. 20, 2003 (Appendix A to Subpart C of Part 164—Security Standards: Matrix).
36. *Supra* note 33.
37. *The Final Security Rule*, 68(34) Federal Register 8343 (Feb. 2003).
38. *Supra* note 33.
39. *Id.*
40. [www.hipaadvisory.com/action/secureqa/secure.htm](http://www.hipaadvisory.com/action/secureqa/secure.htm).
41. J. Root et al., *Field Guide to Implementation* 179 (AMA Press, 2002).
42. *Supra* note 37, at 8361.
43. *National Provider Identifier Confusion*, Am. Prac. Adv. 5 (Feb. 2005).