# Must Schools Comply with the HIPAA Privacy Rule?

By Jill Moore and Aimee Wall

Elementary and secondary schools acquire and maintain a great deal of information about the students they serve. Much of this information is confidential in nature, and parents and students expect the schools to keep it private. At the same time, parents and students expect to have certain rights in the information, such as the right to review it. For over twenty-five years, the Family Educational Rights and Privacy Act (FERPA) has required schools that receive federal funding to protect the privacy of student information and to honor specific rights, including parents' rights to inspect student records and request amendments to them.[1]

One type of confidential information schools maintain concerns their students' health. In North Carolina public schools, each student record contains a "health card" that includes information about such matters as immunization history, significant health problems or medical conditions, and medications taken routinely.[2] Health information about students may also be contained in a variety of other documents, such as individualized education plans or athletic department records. Furthermore, through conversations with students, parents, or health care providers, school personnel may acquire additional health information that is never documented anywhere.

Health care providers who work in schools have long had questions about which of the many confidentiality laws and principles apply to student health information.[3] The focus on this issue has become more intent in recent months because of a new federal regulation governing medical privacy. Most health care providers in the United States were required to comply by April 14, 2003, with the HIPAA Privacy Rule.[4] Because elementary and secondary schools may be served by a variety of health care providers—for example, school nurses, school-based health clinics, and therapists—many people are wondering whether, and how, the Privacy Rule applies to health information in school settings.

Before the HIPAA Privacy Rule was made final, a national task force prepared a set of widely accepted guidelines that urged schools to extend to school health records the same confidentiality protections afforded medical records under state and federal laws.[5] This recommendation highlighted the important issue of whether school health records *should* be protected to the degree imposed by the Privacy Rule, but it did not answer the legal question of whether—and under what circumstances—schools are *required* to apply the rule to protect student health information.

There has been a good bit of confusion on the latter point, some of which is caused by the terms of the rule itself. [6] Just as FERPA regulates only certain information (education records)

---

The authors are School of Government faculty members who specialize in public health law.

1. 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

2. Student's Permanent Health Record, Form No. PPS-2P, in *North Carolina School Health Program Manual*, Section CC: Official Forms (Raleigh: North Carolina Department of Environment, Health and Natural Resources, 1997 and 1999 Supp.).

3. *See, e.g.,* Mary H. B. Gelfman and Nadine C. Schwab, "School Health Records and Documentation," in Nadine C. Schwab and Mary H. B. Gelfman (eds.), *Legal Issues in School Health Services* (North Branch, MN: Sunrise River Press, 2001), 297, which summarizes the issues in two rhetorical questions: "School health records exist because a student has enrolled in a school: does that make them education records? School nurses generate school health records: does that make them health care records?"

4. "HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, sections 262 and 264 (codified at 42 U.S.C. §§ 1320d–1329d-8). The HIPAA Privacy Rule was promulgated by the U.S. Department of Health and Human Services and is found at 45 C.F.R. Parts 160 and 164 (Subpart E). It is one of several regulations implementing HIPAA.

5. National Task Force on Confidential Student Health Information, *Guidelines for Protecting Confidential Student Health Information* (Kent, Ohio: American School Health Association, 2000), 37.

6. *See, e.g.,* Martha Dewey Bergren, "HIPAA Hoopla: Privacy and Security of Identifiable Health Information," *Journal of School Nursing* 17 (Dec. 2001): 336–37: "One question that was not adequately addressed by the final rule . . . is where schools that engage in electronic transactions for third-party reimbursement fit in the picture. . . . Professional experts in both HIPAA and FERPA have differing opinions."

Some commentators have taken the position that schools subject to FERPA are not covered entities under HIPAA. *See, e.g.,* National Association of School Nurses, "Issue Brief: Privacy Standards for Student Health Records" (available at http://www.nasn.org/briefs/hippa.htm; last visited June 11, 2003): "The Final Privacy Rule specifically *excluded* as covered entities schools and universities already covered by the Family Education Rights and Privacy Act

in certain schools (those that receive federal funding), the HIPAA Privacy Rule regulates only "protected health information" created or maintained by "covered entities." The Privacy Rule defines the term "covered entity" in a way that clearly includes some schools but defines "protected health information" in a way that specifically excludes much of the health information that schools maintain. What, then, does this mean for schools that are subject to FERPA? To date, the U.S. Department of Health and Human Services (DHHS) has not clarified this issue. In the absence of DHHS guidance, we believe that school officials should *not* assume that the Privacy Rule does not apply to them.[7] Rather, we would advise school officials to conduct two separate inquiries:

- *The "covered entity" inquiry* Is the school a covered entity as the Privacy Rule defines that term? And, even if the school itself is not a covered entity, are the health care providers who work in the school covered entities?
- *The "protected health information" inquiry* Is any of the health information maintained by the school considered protected health information (PHI) under the Privacy Rule?

This article describes each of those inquiries in detail, using examples from typical North Carolina schools. The flow chart in Figure 1 summarizes the process of determining whether a school or LEA is subject to HIPAA. The article concludes with a brief description of some of the regulatory requirements imposed by the rule.

## The "Covered Entity" Inquiry

The HIPAA Privacy Rule directly regulates three types of "covered entities": [8]

- Health care clearinghouses (entities that help health care providers and health plans standardize electronic health information);
- Health plans (including public and private health insurers, health maintenance organizations, etc.); and
- Health care providers who transmit health information electronically in connection with a HIPAA transaction.

For local education agencies (LEAs) in North Carolina, the covered entity inquiry is twofold. First, the LEA should determine whether any of its activities qualify it as a covered entity. Second, it should assess the activities of others who provide services in the school(s) (but are not part of the LEA's workforce) to determine whether they are covered entities or are part of the workforce of a different organization—such as a local health department—that is itself a covered entity. [9] If the LEA, or anyone providing services within it, is a covered entity, then the management of some student health information may be subject to the Privacy Rule.

### Are LEAs in North Carolina covered entities?

This question requires school officials to consider carefully all the activities of the LEA that are related to health care.

- Is the LEA a health care clearinghouse? In general, a "health care clearinghouse" is an entity that processes health care data into standardized form.[10] It is highly unlikely that the activities of an LEA would bring it within that definition.
- Is the LEA a health plan? An LEA may be responsible for a health plan in some circumstances—if, for example, it provides certain types of group health insurance to its employees.[11] Although this article will not examine the covered-entity status of such health plans, school officials are strongly encouraged to investigate their compliance responsibilities in this regard.
- Is the LEA a health care provider? It is possible—even likely—that an LEA would meet the definition of health care provider under the Privacy Rule.

School officials no doubt think of themselves primarily as providers of education, not health care. However, they cannot

(FERPA)"(emphasis in original). We must disagree with this conclusion, as the definition of "covered entity" does not specify any exclusion. (The ways a school might come within the reach of this definition are discussed in detail below. In contrast, the definition of "protected health information" (see below, "What is PHI?" p. 4) specifically excludes some school records—including those that are education records under FERPA.

7. *See also* Michael Levin and Paul Lalley, "Is the HIPAA Beast Coming to Your School District?" *Inquiry and Analysis,* National School Boards Association Council of School Attorneys, December 2002 (http://nsba.org/site/docs/8800/8709.pdf): "The HIPAA Privacy Rule may affect public school entities in two ways—first, they may have to deal with HIPAA 'covered entities' and second, they may themselves be health plans or health care providers 'covered' by HIPAA."

8. 45 C.F.R. § 160.103.

9. The term "workforce" is defined in HIPAA to include "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity" (45 C.F.R. § 160.103).

10. Specifically, the rule defines a "health care clearinghouse" as a public or private entity (including a billing service, repricing company, community health management information system or community health information system, and a "value added" network or switch) that processes or facilitates the processing of health information from a nonstandard format into a standard format (or vice versa) or from nonstandard data content into standard data content (or vice versa) (45 C.F.R. § 160.103).

11. *See* Aimee Wall, "How Does the HIPAA Privacy Rule Apply to Health Plans in NC Local Government?" (March 11, 2003), available at http://www.medicalprivacy.unc.edu/pdfs/Healthplans.pdf.

avoid providing at least some health care to students. Furthermore, many LEAs employ health care providers, such as nurses or therapists. It is important to recognize, too, that even if the LEA (or someone in its workforce) is a health care provider, the school may not be a covered entity. To be considered a covered health care provider under the Privacy Rule, a person or organization must both

- meet the rule's definition of health care provider, and
- transmit health information electronically, using one of several specific "transactions" regulated by HIPAA.

The first part of this two-part test hinges on the rule's definitions of "health care" and "health care provider." "Health care provider" is defined broadly to include any person who, in the normal course of business, furnishes, bills, or is paid for health care. The term "health care" is also defined quite broadly to include, for example, counseling, physical assessments, and diagnostic, therapeutic, and rehabilitative care.[12] Several different individuals employed by schools could fall within these definitions, including school nurses; psychologists; and physical, speech, and occupational therapists.

The second part of the test depends on whether the health care provider (or the entity employing the provider) transmits health information electronically in connection with one of several health-related transactions specifically regulated by HIPAA (referred to as "HIPAA transactions").[13] One common example of a HIPAA transaction is the claim a health care provider files electronically with a health insurer, such as Medicaid, to obtain payment for services.

*Health care providers must meet both parts of this test to be covered entities.* A person who meets the definition of health care provider but does not transmit health information electronically in connection with a HIPAA transaction is not a covered entity. However, if anyone within an entity (including an LEA) provides health care and conducts associated HIPAA transactions electronically, then the entity itself is considered a covered entity. An entity that contracts with another organization, such as a private billing company, to perform the electronic transactions on its behalf, is also a covered entity.[14]

Many LEAs in North Carolina employ school nurses, and all school nurses satisfy the first part of the two-part test—that is, they meet the definition of health care provider. However, it is uncommon for an LEA or other entity to conduct HIPAA transactions in connection with such conventional school nursing activities as immunization reviews, development of care plans for students with special needs, or assessments of students who are injured or become ill at school.[15] Nevertheless, officials of every LEA that employs a school nurse should confirm whether or not HIPAA transactions, such as electronically transmitting bills to Medicaid for a health care service provided by the nurse, are being conducted. If they are, the LEA is a covered entity.

An LEA may also employ or contract with other health care providers whose status as covered entities should be evaluated. For example, it may employ an occupational therapist who assesses or works with disabled children. Because such a therapist would probably satisfy the definition of health care provider, the key to the covered entity analysis would be the second part of the test: specifically, whether the LEA transmits HIPAA transactions electronically in conjunction with the care provided by the therapist (or, as mentioned above, whether the LEA contracts with a third party to conduct HIPAA transactions on its behalf). An LEA that does so would be considered a covered entity and would have to comply with the Privacy Rule with respect to any PHI that the therapist creates or maintains.[16]

12. The terms are defined in 45 C.F.R. § 160.103.

13. Congress enacted certain portions of the original HIPAA statute to reduce the administrative costs related to the delivery of health care by standardizing the communication of information between health care providers and health plans. As a result, a significant part of the overall HIPAA regulatory regime is devoted to communications between providers, plans, and clearinghouses. The specific HIPAA transactions regulated include transmissions related to: (1) health care claims (or equivalent encounter information), (2) health care payment and remittance advice, (3) coordination of benefits, (4) health care claim status, (5) health plan enrollments and disenrollments, (6) eligibility for a health plan, (7) health plan premium payments, (8) referral certification and authorization, (9) first reports of injury, and (10) health claims attachments. *See* 45 C.F.R. § 164.103.

14. "We note that health care providers who do not submit HIPAA transactions in standard form become covered by this rule when other entities, such as a billing service or a hospital, transmit standard electronic transactions on their behalf. A provider could not circumvent these requirements by assigning the task to its business associate since the business associate would be considered to be acting on behalf of the provider" [Standards for Privacy of Individually Identifiable Health Information: Final Rule, 65 Fed. Reg. 82, 461, 82, 477 (Dec. 28, 2000)].

15. *See* "Roles and Responsibilities of the Nurse in the School Health Program," in *North Carolina School Health Program Manual* (Raleigh: North Carolina Department of Environment, Health, and Natural Resources, 1997 and Supp. 1999).

16. In some circumstances, a therapist or other provider may be hired on a contractual basis. Whether the LEA is considered a covered entity and the therapist classified as part of its workforce will depend on the nature of the contractual relationship and the types of services provided. (*See* note 9 for the definition of "workforce.") If, for example, the LEA bills Medicaid electronically for some of the therapist's services that it is legally obligated to provide to certain students under the Individuals with Disabilities Education Act (20 U.S.C. § 1400 et seq.; 34 C.F.R. pt. 300 et seq.), the LEA, rather than the independent provider, may be considered the "health care provider" under the Privacy Rule. Because DHHS has not provided any guidance regarding this type of arrangement, LEAs need to evaluate their relationships with independent contractors carefully and proceed with caution when determining whether the contractor or the LEA is the covered entity.

When a school system determines that it is a covered entity, its officers should act quickly to assess its obligations under the Privacy Rule, beginning with consideration of the PHI inquiry (discussed below). A covered entity should also carefully consider the option of declaring itself a "hybrid entity." Any covered entity that engages in some activities that are not "covered functions" under HIPAA may elect to designate itself in this way. ("Covered functions" are those functions that make an entity a health plan, health care clearinghouse, or health care provider.[17] ) For example, suppose that an LEA employs a speech therapist who bills Medicaid electronically. This is sufficient to make the LEA a covered entity under HIPAA. But clearly, this activity is only a small part of what the LEA does; most of its work—the provision of education—does not meet HIPAA's definition of a covered function. The hybrid entity designation permits the LEA to apply the Privacy Rule only to its "health care component," that is, the activities that make it a covered entity. (See "What is a 'Hybrid Entity'"? p. 6.) If the LEA determines that it is a covered entity and does not designate itself a hybrid entity, *all* PHI within its control becomes subject to the Privacy Rule.

### Are outside health care providers associated with LEAs covered entities?

An LEA that does not employ or contract with anyone who qualifies as a covered health care provider may still be affected by the Privacy Rule if "outside" health care providers who are covered entities work in the schools. For example, many school systems in North Carolina are served by school nurses employed by the local health department. All local health departments in North Carolina bill Medicaid electronically, which is sufficient to make them covered entities under the Privacy Rule. Therefore, school nurses who work for a health department could be considered part of the workforce of a covered entity.[18] If they are, and if the health department does not designate itself a hybrid entity and exclude the school nursing program from its health care component, school nurses will have to comply with the Privacy Rule with respect to any PHI they maintain. (See the discussion below regarding what information qualifies as PHI.) A health department that *is* a hybrid entity may exclude the school nursing program from its health care component as long as it conducts no HIPAA transactions in connection with the program. A similar analysis applies to a school nurse employed by a local hospital that is a covered entity.

Some LEAs are also associated with a school-based health center whose status as a covered entity should also be evaluated. Such centers present perhaps the most straightforward analysis of all the health care providers associated with schools: all school-based health centers in North Carolina meet the definition of health care provider. And, as they probably all bill Medicaid and other insurers electronically for services provided to students, it is very likely that all school-based health centers in North Carolina are covered entities.[19]

## The "Protected Health Information" Inquiry

Once an LEA determines that it is a covered entity, or that it is served by a covered entity (or a covered health care component of a hybrid entity), the next step is to determine whether the covered entity or component creates or maintains any protected health information (PHI). The Privacy Rule applies only to information maintained by a covered entity that meets the definition of PHI.

### What is PHI?

The Privacy Rule defines PHI as health information in any form or medium—including oral, paper, and electronic information—that identifies an individual and relates to one of the following: (1) the individual's past, present, or future physical or mental health or condition; (2) the provision of health care to the individual; or (3) past, present, or future payment for health care provided to the individual.[20] A few categories of information are specifically excluded from the definition of PHI, including two types of student records:

- Education records covered by FERPA; and
- Records of students held by postsecondary educational institutions or records of students eighteen years of age or older when those records are used exclusively for health care treatment and have not been disclosed to anyone other than a health care provider at the student's request.[21]

17. 45 C.F.R. § 164.103.

18. When an individual is employed by one entity but performs work for another, to which workforce does he or she belong—the employer's or the other entity's? HIPAA's definition of "workforce" (see note 9) does not answer this question, and DHHS has provided no specific guidance on this issue. Our discussion assumes that a school nurse employed by a local health department is a member of that department's workforce even when working in a school. However, it is possible that DHHS or a court would conclude that the nurse is a member of the school's workforce while performing school nursing duties—or even is a member of both workforces. The determination would probably depend on whether DHHS considers the nurse to be working "under the direct control of" the school, the health department, or both.

19. The only exception would be a school-based health center that does not engage in electronic billing or any other electronic HIPAA transaction. The authors are not aware of any school-based health center in North Carolina that does not bill Medicaid electronically.

20. 45 C.F.R. § 160.103.

21. The only other exception to the definition of PHI is for "employment records held by a covered entity in its role as employer" (45 C.F.R. § 160.103).

Even though these two types of records usually contain individually identifiable health information, such as immunization information, DHHS explicitly decided not to regulate them under the Privacy Rule. In a commentary accompanying the rule, DHHS explained that the first exclusion—education records covered by FERPA—was appropriate because these records are already subject to a comprehensive regulatory scheme that balances the confidentiality and access interests of schools, parents, and students. Additional regulation of these education records is therefore unnecessary.[22]

The second exclusion from the definition of PHI—treatment records of older students—is a little more complicated. As these records are also excluded from the definition of education record in FERPA, they are subject to neither FERPA nor HIPAA. DHHS explains the reasoning behind the exclusion from HIPAA this way:

> Because FERPA excludes these records from its protections *only to the extent they are not available to anyone other than persons providing treatment to students*, any use or disclosure of the record for other purposes, including providing access to the individual student who is the subject of the information, would turn the record into an education record. As education records, they would be subject to the protections of FERPA.[23]

In other words, once these treatment records are made available to anyone for purposes other than treatment, they lose their exclusion from the definition of PHI. In a school subject to FERPA, these treatment records would then be regulated by FERPA. In a school *not* subject to FERPA—but in which the school (or a provider working in the school) *is* a covered entity—these treatment records would be considered PHI and would be regulated by the Privacy Rule. Nonetheless, DHHS evidently concluded that, as this type of information would in any case only be used by and disclosed to a restricted group of people for limited, treatment-related purposes, the additional privacy protections and administrative burdens of the Privacy Rule were unnecessary and could only create confusion.

### Given these broad exclusions, do schools have any PHI?

Most schools or school-based providers that meet the definition of covered entity are likely to have some information considered PHI—including schools subject to FERPA. Schools that are not subject to FERPA (for example, private schools not receiving federal funding) but that are covered entities under HIPAA are likely to have a significant amount of PHI, because they are not able to take advantage of the exclusion of education records from the definition of PHI. School-based health centers are also likely to have a significant amount of PHI, because the records they generate—even in schools subject to FERPA—are generally not considered education records. Such records are not subject to FERPA because the centers typically are not part of the school or the LEA but are operated by a separate legal entity (such as a local health department) that contracts with the LEA to provide student health services. The contract typically specifies that the center's records are not subject to FERPA; and because they are not education records subject to FERPA, they are not excluded from the definition of PHI under the first exception. Therefore, the center's records *do* contain PHI and the center *does* need to comply with the Privacy Rule with respect to that PHI.[24]

Despite the two broad FERPA-related exceptions to the definition of PHI, even schools subject to FERPA (including all public elementary and secondary schools in North Carolina) may create and maintain some PHI. The commentary accompanying the exclusions strongly suggests that DHHS did not wish to impose the Privacy Rule's complex regulatory scheme unnecessarily on health information in schools that are subject to FERPA. For the most part, excluding education records covered by FERPA from the definition of PHI achieves this goal. As a result of that exclusion, most of the records acquired or maintained by a school nurse—for example, students' immunization records or notes about health care provided to students at school—would fall within FERPA's definition of education record and so would not be subject to the Privacy Rule.[25] However, if DHHS intended to

Although the term "employment record" is not further defined, DHHS has explained that "medical information needed for an employer to carry out its obligations under FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance and fitness-for-duty tests of employees, may be part of the employment records" when held in the entity's role as employer (rather than its role as a health care provider) [Standards for the Privacy of Individually Identifiable Health Information: Final Rule, 67 Fed. Reg. 53,182, 53,192 (Aug. 14, 2002)].

22. Under FERPA, the term "education records" means "those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution." Four specific types of records are excluded from the definition of "education records": certain sole possession notes, records of law enforcement units of the education agency or institution, employment-related records, and treatment records of older students. 20 U.S.C. § 1232g(a)(4)(A & B).

DHHS explained in a commentary accompanying the Privacy Rule that it "excluded education records covered by FERPA . . . because Congress specifically addressed how information in education records should be protected" [65 Fed. Reg. 82,483 (Dec. 28, 2000)].

23. 65 Fed. Reg. 82,483 (emphasis added).

24. The only exceptions are certain records (employment records and treatment records of older students) covered by the other two exclusions from the definition of PHI. *See* 45 C.F.R. § 164.103 (definition of PHI).

25. There is some confusion about which records maintained by a school nurse are subject to FERPA. A document, file, or record is an education record

completely exempt from the rule *all* health information maintained by schools subject to FERPA, it drew too narrow an exclusion.

First, the exclusion does not take into account all oral communications of health information that may occur within the school. FERPA applies to information contained in records, files, documents, and other similar materials and to the oral communication of that information; but it does not extend to oral communications of information that is not contained in some sort of record. Thus, any oral communication of health information that is *not* part of an education record (as defined by FERPA) meets the definition of PHI. Therefore, in an LEA that is a covered entity, oral communications of health information that are not maintained in an education record are subject to the Privacy Rule.

Second, the exclusion from the definition of PHI for records covered by FERPA also fails to take account of a significant category of school records that may contain health information: "sole possession notes." Under FERPA, notes made by a member of the school's staff that are not accessible or revealed to any other person (other than the staff member's substitute) are excluded from the definition of education record.[26] These sole possession notes are therefore *not* subject to FERPA, though they are PHI and so subject to the Privacy Rule if maintained by a covered entity or a member of a covered entity's workforce.[27] It is not known whether DHHS

*Continued on p. 8*

under FERPA if it "(i) contain[s] information directly related to a student; and (ii) [is] maintained by an educational agency or institution, *or by a person acting for the agency or institution*" [20 U.S.C. § 1232g(a)(4)(A) (emphasis added)]. School nurses are persons acting for the school; thus, documents that they create that contain information directly related to a student are education records under FERPA unless they fit into one of the exceptions to the definition of education records, such as sole possession notes (see note 26 and accompanying text). It is important to note that the definition of "education record" does not hinge on where the document is located or maintained. Health information need not be on the health card or maintained in the student's school file to be considered an education record. Many school nurses document some student information in notebooks or files that are portable and may be maintained somewhere other than the school. For example, a school nurse employed by the local health department might maintain student files there. Such documents are nevertheless education records subject to FERPA, unless they fit into an exception.

26. 20 U.S.C. § 1232g(a)(4)(B)(iii) excludes "records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute."

27. *See also* Michael Levin and Paul Lalley, "What to Do When the HIPAA Beast is at Your Door," *Inquiry and Analysis,* National School Board Association Council of School Attorneys, January 2003 (http://www.nsba.org/site/docs/9300/9258.pdf), noting that FERPA's definition of "education records" excludes sole possession notes. They conclude, therefore, that "the individual notes of a physical therapist or a school psychologist about a student are not records protected by FERPA but might be governed by HIPAA if the school district were a covered entity." Sole possession notes are not, however, PHI if they fall within the PHI exclusion for the treatment records of older students.

## What Is a Hybrid Entity?

The HIPAA Privacy Rule applies to a broad range of entities, including some that may perform only one or a few of the functions that qualify them as covered entities. For example, a large manufacturing company may provide some on-site health care to its employees. If the company's health clinic meets the definition of a covered entity (i.e., it is a health care provider conducting HIPAA transactions electronically), the company will have to comply with the Privacy Rule with respect to any protected health information (PHI) that it creates or maintains. In drafting the rule, DHHS recognized that larger, more diversified organizations—such as this manufacturing company—might wish to limit their compliance responsibilities so that only certain parts of the organization are required to comply with the Privacy Rule. DHHS therefore created the concept of a "hybrid entity."

A covered entity may choose to designate itself a hybrid entity if it is a single legal entity that carries out functions that are not covered functions. (Covered functions are those activities or functions that make the entity a health plan, health care clearinghouse, or health care provider.)[i] In other words, the entity must perform some functions that, if performed by freestanding legal entities, would not qualify that entity as a covered entity. For example, the large manufacturing company that has an employee health care clinic covered by HIPAA might also offer employees, as a separate program, a free single-parent support group directed by a family therapist. The family therapist would undoubtedly be considered a "health care provider"; but, because the services are free, no HIPAA transactions are associated with the support group. Unless the company designates itself a hybrid entity and excludes the support group from the covered health care component, the information generated in those group meetings and the records maintained by the therapist could be considered PHI; if so, they would be subject to all the requirements of the Privacy Rule. If the company designates itself a hybrid entity, it can limit the applicability of the rule to the PHI created and maintained by the health care clinic.

As the following examples demonstrate, the hybrid entity concept is useful in school settings because it allows schools to limit the number of people and records that are subject to the Privacy Rule.

> **Example 1.** A small school employs only one health care provider—a speech therapist. The therapist satisfies the two-part test for a covered health care

i. 45 C.F.R. § 164.103 (definitions of hybrid entity and covered functions); § 164.105 (requirements applicable to hybrid entities).

provider (see p. 3) because the school bills Medicaid electronically for some of the services she provides. As a result, the school is a covered entity. In this situation, the school may want to designate itself a hybrid entity to ensure that the Privacy Rule applies only to information about the therapist's activities—not to any other health information the school maintains.[ii]

**Example 2.** A public school nurse is employed by a local health department and provided to the school through an informal agreement with the LEA. The health department is covered by HIPAA because, among other things, it has a prenatal clinic that provides health care for which it electronically bills Medicaid and other insurers. However, the health department has the option of designating itself a hybrid entity because it performs other functions, such as restaurant inspections, that are not covered functions. The school nurse the health department employs does not bill Medicaid or any other insurer nor conduct any other HIPAA transactions in his role as a school nurse. If the local health department designates itself a hybrid entity, it can choose to exclude the school nurse from its health care component so that the nurse will not have to comply with the Privacy Rule.

How does a covered entity go about designating itself a hybrid entity? The Privacy Rule simply requires that the entity identify its "health care components" (i.e., those components that will comply with the rule) and document its decision to designate itself a hybrid entity.[iii] The covered entity is not required to submit any documentation to DHHS, or to take any other formal steps in order to be considered a hybrid entity. The entity must, however, review its operations carefully to determine exactly which components should be considered health care components and which employees should be included within each health care component. Specifically, any component that would be a covered entity if it were a separate legal entity (such as a health care provider that bills insurers electronically) *must* be included in the health care component. The rule outlines additional guidelines for other components that may be included in the health care component. For example, the entity may choose to include components that are health care providers even if they do not bill insurers electronically.

In documenting its hybrid entity status and health care components, a covered entity may want to explain why it elected to include certain components and not others. The rule does not require this level of detail, though such an explanation will provide guidance for the entity's future leaders in the event that they ever face a compliance review by the federal government or decide to reassess the entity's status under HIPAA.

The identification of health care components is an important step because, once they are identified, health care components must behave—in respect to sharing PHI—as if they were legal entities separate from the rest of the covered entity. Once an entity is identified as a hybrid entity, any sharing of information from a health care component to a non–health care component is a "disclosure" and must comply with the Privacy Rule's restrictions regarding disclosure. The rule requires covered entities to put in place specific safeguards to prevent inappropriate sharing of PHI between components of the same organization. In addition, the rule recognizes that some employees may perform functions for both health care and non–health care components and prohibits those employees from using PHI from the health care component in any of the work they perform in the non–health care component in most circumstances.[iv] Consider, for example, the school nurse above who is employed by the health department. If he works three days each week at the school and two days in the prenatal clinic, he needs to be trained to comply with the Privacy Rule when working at the clinic but not when working at the school. He would also need to exercise caution when using information learned as a prenatal clinic nurse during his work as a school nurse, to ensure that he does not use any information he is not authorized to have in his school nurse role. In other words, unless the Privacy Rule authorizes the disclosure of the information from the clinic to the school, the information should not be available for him to use within the school. This could mean he must act as if he does not know the information while working as the school nurse.

While a hybrid-entity designation requires some additional administrative effort on the part of covered entities, it allows such entities to significantly reduce their compliance responsibilities under the Privacy Rule. Schools that are covered entities or that are associated with covered entities should carefully consider the benefits of a hybrid-entity designation as they move forward with their compliance efforts.

ii. The example is for illustration only. An LEA may have multiple health care providers on staff and may also be responsible for a "health plan" that qualifies as a covered entity.

iii. 45 C.F.R. § 164.105(a)(2)(iii); 164.530(j).

iv. *Id.* at § 164.105(a)(2)(ii).

## Must an LEA Comply with HIPAA?

Is the LEA (or any member of its workforce) a health plan, health care clearinghouse, or health care provider that transmits health information electronically in connection with a HIPAA transaction?

**Yes** → The LEA is a covered entity subject to HIPAA. PHI[a] it creates or maintains is subject to the Privacy Rule. The LEA may limit applicability of the Privacy Rule by designating itself a hybrid entity.[b]

**No** → The LEA itself is not a covered entity but may still be affected by the Privacy Rule.

Is any individual who performs work on the LEA's behalf a covered entity or a workforce member of a covered entity?

**Yes** → HIPAA applies to such individuals. PHI they create or maintain is subject to the Privacy Rule unless the individual works for a covered entity that can and does designate itself a hybrid entity and excludes those who work in the LEA from its health care component.

**No** → These individuals are not subject to HIPAA. The health information they create or maintain is not subject to the Privacy Rule.

a. See p. 4, "What is PHI?"
b. See p. 6, "What Is a Hybrid Entity?"

*Continued from p. 6*

gave any consideration to exempting sole possession notes from the definition of PHI; but if it *had* done so, it seems likely that it would have exempted the notes from the definition of PHI for the same reason it exempted the treatment records of older students: if a sole possession note is shared with another person (other than a substitute), it immediately becomes an education record subject to FERPA. It thus seems incongruous that DHHS would intentionally impose the complex regulatory requirements of the Privacy Rule on a class of information (sole possession notes) that is already, by definition, extraordinarily private.

Unfortunately, the current version of the regulation does not provide exemptions for oral communication of health information not contained in education records, nor for the sole possession notes of health care providers working in schools. The frustrating result is that a covered health care provider working in a school, such as a school nurse, may be forced to comply with FERPA for most records and for oral communications about information in those records but with the Privacy Rule for other oral communications and for sole possession notes.

### What Does the Privacy Rule Require Covered Entities To Do?

The Privacy Rule requires covered entities to comply with rigorous and detailed new guidelines.[28] There are three basic components to this new regulatory regime. First, when using and disclosing PHI, a covered entity must abide by detailed requirements applicable to a variety of different circumstances. They specify, for example, when a covered entity may use and disclose PHI to provide treatment to an individual (e.g., a student) and when it may do so to obtain payment for that treatment. The rule also specifies when a covered entity may disclose PHI to law enforcement officials, public health authorities, researchers, and a variety of other groups that often seek confidential medical information to support their activities.[29]

The second fundamental component of the Privacy Rule is a set of new individual rights with respect to health information. For example, patients of covered entities now have a federal right to inspect and obtain copies of their records and to have inaccurate or incomplete records amended. A patient also has the right to receive a written copy of a notice describing how the covered entity uses and discloses PHI.[30]

Third, and finally, the rule imposes a series of new administrative requirements on covered entities. Entities must, for example,

- appoint a privacy official to oversee the entity's compliance with the Privacy Rule,
- provide training to workforce members who have access to PHI,
- maintain a system to receive complaints from patients about privacy practices, and

28. Institute of Government faculty members have developed detailed outlines describing the requirements of the Privacy Rule and additional materials to help public agencies comply with the rule. Those materials are available on the Internet at http://www.medicalprivacy.unc.edu.

29. 45 C.F.R. § 164.502(a); § 164.506; § 164.512. In North Carolina, a number of state laws govern use and disclosure of health information as well. For a partial inventory of those laws, see http://www.nchica.org/HIPAAResources/Samples/statesort.pdf.

30. 45 C.F.R. §§ 164.524; 164.526; 164.520.

- develop comprehensive written policies and procedures related to all the rule's requirements.[31]

As almost all covered entities were required to be in compliance with the Privacy Rule by April 14, 2003, enforcement activities are now possible.[32] DHHS has delegated responsibility for these activities to the DHHS Office for Civil Rights, explaining that "[e]nforcement activities will focus on obtaining voluntary compliance through technical assistance. The process will be primarily complaint driven and will consist of progressive steps that will provide opportunities to demonstrate compliance or submit a corrective action plan."[33]

Under the statutory authority provided in HIPAA, DHHS may impose civil monetary penalties of $100 for each violation and up to $25,000 per year for all violations of an identical requirement or prohibition. In addition, the legislation provides for criminal penalties for some violations ranging from $50,000 and/or one year in prison to $250,000 and/or ten years in prison.[34]

## Conclusion

The presence of health care providers in schools raises the question of whether student health information is subject to the HIPAA Privacy Rule. Although DHHS may have intended to create a complete exemption from the rule for schools covered by FERPA, the rule failed to take into account certain classes of information—such as sole possession notes and some oral communications—that may be considered PHI. As a result, school nurses and others in North Carolina's public elementary and secondary schools may find themselves in the strange situation of having to apply FERPA's requirements to most of their records and information but the Privacy Rule's requirements to others.

The Privacy Rule applies only if the school, or the health care provider working in the school, is a covered entity. Health care providers who transmit health information electronically in connection with a HIPAA transaction are covered entities. But even health care providers who do not conduct HIPAA transactions in connection with health care provided in the school are subject to the Privacy Rule if they work for a covered entity. This result can be avoided if the health care providers' employer takes specific steps to designate itself a hybrid entity and excludes providers' school work from coverage by the rule.

Because the compliance date for the Privacy Rule has passed, schools that have not already determined their potential exposure under the rule should act quickly to do so. Each school or LEA should first determine whether it is a covered entity—either as a health care provider or a health plan. If it is a covered entity, it should take the following steps:

1. Determine whether it should be a hybrid entity and, if appropriate, identify its health care components and prepare the appropriate documentation.
2. Appoint and educate a privacy official for the entity (one person responsible for implementation of the rule).
3. Identify PHI within the entity's health care components and evaluate how that information is being used within the entity and disclosed to others.
4. Develop written policies and procedures for the use and disclosure of PHI that are consistent with the Privacy Rule and all other applicable laws and implement safeguards to prevent PHI from being used and disclosed in violation of those policies and procedures.
5. Develop the documentation needed to comply with the requirements of the Privacy Rule, including a written notice of privacy practices and authorization forms.
6. Identify the entity's "business associates"[35]—other entities that use PHI to perform functions on behalf of the covered entity—and, where appropriate, enter into business associate agreements with those entities.
7. Train staff of the entity's health care components in their obligations under the Privacy Rule.

Because the detailed requirements of the Privacy Rule can be intimidating, schools subject to the rule should consider forming regional workgroups or otherwise collaborating with other schools to develop forms, policies, and procedures to ease the burdens of compliance. ■

31. 45 C.F.R. § 164.530.

32. Small health plans regulated by HIPAA have an additional year (until April 2004) to come into compliance with the Privacy Rule. 45 C.F.R. § 164.534(b)(2). A "small health plan" is a health plan with annual receipts of $5 million or less. *Id.* at § 160.103.

33. DHHS Press Release, "CMS Named to Enforce HIPAA Transaction and Code Sets Standards; HHS Office of Civil Rights to Continue to Enforce Privacy Standards" (Oct. 15, 2002), available at http://www.hhs.gov/news/press/2002pres/20021015a.html (last visited June 19, 2003). *See also* 65 Fed. Reg. 82,472 (Dec. 28, 2000) (DHHS commentary explaining that enforcement activities will focus on voluntary compliance by providing technical assistance and guidance as well as "investigating complaints and conducting compliance reviews; and, where voluntary compliance cannot be achieved, seeking civil monetary penalties and making referrals for criminal prosecution"). Members of the public may submit complaints about a covered entity's privacy practices by mail or fax to the regional offices of the Office of Civil Rights (listed on the Internet at www.hhs.gov/ocr/regmail.html) or by e-mail at OCRComplaint@hhs.gov (last visited June 19, 2003).

34. 42 U.S.C. §§ 1176, 1177; *see also* Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings: Interim Final Rule, 68 Fed. Reg. 18,895 (April 17, 2003).

35. *See* 45 C.F.R. § 160.103 (definition of "business associate"); 45 C.F.R. §§ 164.502(e), 164.504(e) (requirements applicable to business associates).