Applicability of HIPAA to
Health Information in Schools

Jill Moore and Aimee Wall*
UNC School of Government

I. What is HIPAA? What is the privacy rule?

A. HIPAA: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the U.S. Department of Health and Human Services (U.S. DHHS) to develop a series of rules governing health information. In general, the rules are intended to standardize the communication of electronic health information between health care providers and health insurers. In addition, the rules are intended to protect the privacy and security of individually identifiable health information. Several of the HIPAA rules have been published in proposed form and three rules, including the privacy rule, have been published in final form.

B. The HIPAA Privacy Rule (Code of Federal Regulations, Title 45, Part 164): The HIPAA privacy rule governs how "covered entities" may use and disclose "protected health information." The requirements of the privacy rule are summarized in Section VI below. Health care providers who are regulated by HIPAA must comply with the privacy rule by April 14, 2003.

II. Who is regulated by the HIPAA privacy rule?

A. "Covered entities" are regulated: HIPAA directly regulates the following three types of "covered entities":

1. Health plans (insurers, HMOs, Medicaid, etc.);

2. Health care clearinghouses (entities that help health care providers and health plans standardize their health information); and

3. Health care providers who transmit health information in electronic form in connection with a HIPAA transaction. It is important to recognize that there is a two-part test for determining whether an entity is a covered health care provider:

* Much of the material in this outline was originally prepared by Jill Moore. Aimee Wall adapted and supplemented the material specifically for the 2003 School Attorneys' Conference.

a. Part one: Is the entity a "health care provider" as that term is defined by HIPAA? "Health care provider" is defined as any person who, in the normal course of business, furnishes, bills, or is paid for "health care." The term "health care" is defined quite broadly to include preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling, service, assessment, or procedure with respect to the physical and mental condition, or functional status of an individual or that affects the structure or function of the human body.

b. Part two: Does the entity transmit health information in electronic form in connection with a HIPAA transaction? HIPAA transactions are exchanges of information between two parties to carry out financial or administrative activities related to health care, including transactions such as filing a health insurance claim with an insurer and determining eligibility for health insurance.

B. School nurses, school-based health clinics, and local education agencies (LEAs) may be regulated by the HIPAA privacy rule. The activities of school nurses and school-based health clinics are easily recognized as traditional health care activities and, as such, should be closely examined under HIPAA to determine if they are "covered entities." The applicability of HIPAA to school-based health clinics is discussed in detail in Section IV below and the applicability of HIPAA to school nurses is discussed in Section V. Above and beyond the activities of the nurses and clinics, however, LEAs may be engaging in other activities that qualify the LEA as a "health care provider" under the HIPAA definition. For example, an LEA employee may conduct hearing assessments or provide health-related services to a disabled student. If the LEA also conducts one or more HIPAA transactions electronically in order to, for example, obtain payment for that service from a third-party payer (such as Medicaid), the LEA would become a covered entity under HIPAA.

III. <u>What information is regulated by the HIPAA privacy rule?</u>

A. "Protected health information" is regulated: The HIPAA privacy rule requires covered entities to protect the privacy of "protected health information" (PHI). PHI is defined as information held or disclosed by the covered entity in any form (electronic, paper records, oral communications) that:

1. Identifies an individual, and
2. Relates to:
   a. the individual's past, present, or future physical or mental health or condition;
   b. the provision of health care to the individual; or
   c. the past, present, or future payment for the provision of health care to the individual.

B. Exceptions to the definition of PHI: The term "protected health information" has several specific exceptions that are particularly relevant to health information in schools. Specifically, the term does not include:

1. Education records covered by FERPA: This is a very significant exception for schools to consider. If the information falls within the FERPA definition of "education record" (20 U.S.C. 1232g(a)), it will not be considered PHI under HIPAA (and therefore will not be regulated by HIPAA).

2. Certain records excluded from the definition of "education record" in FERPA: Specifically, the term "protected health information" excludes records of students held by post-secondary educational institutions or of students 18 years of age or older, used exclusively for health care treatment and which have not been disclosed to anyone other than a health care provider at the student's request.

3. Employment records held by a covered entity in its role as employer: The term "employment record" is not defined further in the rule but the U.S. DHHS explained in guidance 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). 67 Fed. Reg. 53,192 (August 14, 2002).

IV. School-based health clinics: Are they "covered entities" under HIPAA? Do they maintain or communicate "protected health information"?

A. Are school-based health clinics "covered entities" under HIPAA? As discussed above, if a health care provider transmits health information electronically in connection with a HIPAA transaction, the provider is a "covered entity." School-based health clinics meet this two-part test and therefore are covered entities. In sum,

1. All school-based health clinics are "health care providers" as that term is defined by HIPAA.

2. It is our understanding that all school-based health clinics transmit health information electronically in connection with a HIPAA transaction. For example, the clinics may file a claim electronically with Medicaid for health care services provided to a student.

B. Is the health information maintained or communicated by school-based health clinics "protected health information"?

1. Most of the information maintained by clinics would meet the general definition of PHI. In other words, they maintain individually identifiable information that relates to an individual's health, health care or payment for health care.

2. The information maintained by school-based health clinics will most likely not fall within the FERPA exception to the definition of PHI. School-based health clinics are typically created by contractual arrangements between local education agencies and a health care provider (often the local health department). The contract should specify that the records and information of the school-based health clinic are separate from and not a part of the educational record as defined by FERPA. Because the clinic's records are not subject to FERPA, they are not excepted from the definition of PHI.

V. Schools nurses under HIPAA: Are they "covered entities" under HIPAA? Do they maintain or communicate "protected health information"?

A. Are school nurses covered entities under HIPAA? School nurses are health care providers, as that term is defined by HIPAA. However, health care providers are regulated by HIPAA only if they transmit health information electronically in connection with a HIPAA transaction. To determine if a school nurse is a covered entity, answer the following questions:

1. Does the school nurse, as part of her school nursing work, ever transmit health information electronically in connection with a HIPAA transaction?
   a. If the answer is yes, the nurse is covered—stop here.
   b. If the answer is no, the nurse still may be covered—proceed to question 2, below.

2. Does the school nurse's employer ever engage in HIPAA-covered transactions?
   a. If the school nurse is employed by an entity that never transmits health information electronically in connection with a HIPAA transaction, the nurse is not covered—stop here.

i. Example: If an LEA employs a school nurse, one would need to determine whether the LEA ever transmits health information electronically in connection with a HIPAA transaction—either in connection with the nurse's work, or with other activities of the LEA, such as speech and hearing assessments that are billed to Medicaid. If the LEA never transmits health information electronically in connection with a HIPAA transaction, the nurse is not covered by HIPAA and the analysis concludes here. However, if any activity of the LEA results in the electronic transmission of health information in connection with a HIPAA transaction, the nurse may be covered—proceed to question 3.

b. If the school nurse is employed by an entity that does transmit health information electronically as part of her school nursing work, she still may be covered—proceed to question 3, below.
   i. Example: All local health departments in North Carolina are regulated by HIPAA because they all are health care providers transmitting health information electronically in connection with a HIPAA transaction. If the health department employs a school nurse, the nurse may be covered, depending upon the answer to question 3, below.

3. Has the school nurse's employer taken action to exclude the school nursing program from HIPAA coverage? That is, has it (1) determined that it is a "hybrid entity," (2) designated the programs, activities, and functions that make up its "health care component," and (3) determined that the school nursing program is *not* part of its health care component?

   a. If the employer is a covered entity that has not taken these actions, the school nurse is covered by the HIPAA privacy rule.

   b. If the employer has (1) determined that it is a hybrid entity, (2) designated its health care component, and (3) excluded the school nursing program from its health care component, the school nurse is *not* covered by HIPAA.

   c. If the employer has (1) determined that it is a hybrid entity, (2) designated its health care component, and (3) included the school nursing program in its health care component, the school nurse is covered by HIPAA.

4. What did question 3 mean? What are these things—hybrid entities and health care components?

    a. Some covered entities can exclude some of their programs and operations from being covered by HIPAA. 45 C.F.R. § 164.504(a)-(c). To do so, they must take all the following steps:

        i. The covered entity must determine that it is a "hybrid entity." This means that it has some functions or activities that do not meet the definition of covered entity.
            (1) Example: Local health departments have septic tank inspection and permitting programs. These programs do not meet the definition of covered entity, because they are not health plans, health care clearinghouses, or health care providers. Therefore, local health departments may be hybrid entities.

        ii. The covered entity must designate, in writing, which of its programs, activities, or functions make up its "health care component." It must include in this designation any program, activity, or function that meets the definition of covered entity. It may choose whether or not to include programs, activities, or functions that do not meet the definition of covered entity.
            (1) Example: Local health departments have prenatal clinics that provide health care and bill Medicaid electronically. These clinics must be included in the health department's health care component because they meet the definition of covered entity.
            (2) Example: Local health departments have septic tank inspection and permitting programs. These programs are not required to be included in the health department's health care component because they do not meet the definition of covered entity.
            (3) Example: A local health department provides school nurses to the school system. This particular school nursing program does not transmit health information electronically in connection with a HIPAA transaction. The health department may choose whether or not to include the school nursing program in its designation of health care component.

        iii. After a covered entity completes this process, it must ensure that all programs, activities, and functions in its health care component comply with the privacy rule. Programs, activities, or functions that are not part of the health care component do not have to comply with the privacy rule.

(1) Example: A local health department has designated its school nursing program as part of its health care component. The school nurses must comply with the privacy rule.

(2) Example: A local health department has excluded the school nursing program from its health care component. The school nurses are not required to comply with the privacy rule. For purposes of HIPAA compliance, the health department's health care component must treat the school nursing program as if it were a separate legal entity when sharing PHI.

B. Is the health information maintained or communicated by school nurses covered by HIPAA?

1. Is the school nurse a covered entity under HIPAA?
   a. If the answer is no, the school nurses' information is not covered by HIPAA—stop here.
   b. If the answer is yes, some of the school nurses' information may be covered by HIPAA—proceed to question 2, below.

2. Is the health information maintained or communicated by the school nurse part of the education record under FERPA?
   a. Health information that is part of the education record under FERPA is not covered by HIPAA.
   b. Any health information that is <u>not</u> part of the education record and that is maintained by a nurse who is a HIPAA covered entity is covered by HIPAA.

VI. <u>If a school program or activity is regulated by HIPAA, what must it do to comply with the privacy rule?</u>

A. Privacy rule requirements: The privacy rule requires covered entities to comply with many different requirements that will supplement and modify each entity's current health privacy practices. In sum, the rule requires the entity to (1) use and disclose PHI only as provided in the rule, (2) honor several new individual rights with respect to health information, and (3) adhere to several basic administrative requirements. Each of these three general sections of the rule is briefly summarized below.

B. Framework for use and disclosure

1. General rule: Covered entities may not use or disclose PHI except as required or permitted by the privacy rule. § 164.502(a).

a. Required disclosures:

i. Compliance: The rule requires covered entities to disclose PHI in response to a request from DHHS in order to monitor compliance with the privacy rule. § 164.502(a)(2).

ii. Individual: The rule requires covered entities to disclose PHI to the individual upon request (i.e., to the patient or health plan enrollee or his or her personal representative). §§ 164.502(a)(2)(i); 164.524; 164.528.

b. Permitted uses and disclosures

(1) For treatment, payment and health care operations: Covered entities are permitted but are not required to obtain an individual's written permission (or "consent") to use and disclose PHI for treatment, payment and health care operations in certain circumstances. § 164.506.

ii. With individual permission: The privacy rule permits covered entities to disclose PHI subject to an individual's written authorization. The rule outlines several requirements relating to the content of the authorization and also imposes certain restrictions on covered entities obtaining authorizations to ensure that the authorizations are voluntary. For example, a covered entity may not condition the provision of treatment to a patient upon obtaining an authorization except in very limited circumstances. The privacy rule also permits uses and disclosures pursuant to "implied" permission – for example, if an individual fails to object when a provider discusses PHI in the presence of a family member or close friend of the individual. (See Botts outline[1] "Using and Disclosing PHI with Individual Permission").

iii. Without individual permission: The privacy rule outlines several different circumstances in which a covered entity may disclose (and sometimes use) PHI without the individual's permission. For example, covered entities may disclose information to public health officials, law enforcement officials and researchers if certain conditions are satisfied. (See Moore outline "Using and Disclosing Information Without Individual Permission Pursuant to Privacy Rule § 164.512").

[1] Other outlines referenced in this outline are available at http://www.medicalprivacy.unc.edu.

iv. Pursuant to a data use agreement: Covered entities may use and disclose a "limited data set" for public health, research or health care operations purposes if the entity enters into a data use agreement with the recipient of the data set. § 164.514(e).

2. Minimum necessary: When using or disclosing PHI and when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. § 164.502(b). There are several exceptions to the minimum necessary requirement and detailed compliance requirements. (See Moore outline "Minimum Necessary").

3. Incidental disclosures: A covered entity will not be in violation of the rule if PHI is used or disclosed <u>incident to</u> a permitted use or disclosure as long as (1) reasonable and appropriate safeguards are in place and (2) the entity complies with the minimum necessary requirement. § 164.502(a)(1)(iii). In other words, a covered entity will not be in violation of the rule for uses or disclosures that are "by-products" of acceptable uses and disclosures.
   a. Example: A physician may use a sign-in sheet in order to check people in for appointments. This "use" is permitted under the privacy rule as part of treatment. However, when one patient signs in, he or she is able read the names of the other patients listed on the sign-in sheet. This "disclosure" of patient names to other patients is not considered part of treatment but it would be permitted as a disclosure that is "incident to" a permitted use (i.e., the physician's receptionist and nurse using the sign-in sheet in order to treat each patient). The physician must use "reasonable safeguards" which means, for example, that the sign-in sheet should not require each patient to list "reason for visit," "symptoms," or "diagnosis."

C. Individual Rights

1. Notice: Individuals have the right to receive a written notice describing the covered entity's privacy practices. This notice is a comprehensive inventory of how the entity uses and discloses PHI as well as an explanation of the individual's rights with respect to PHI. Except in emergency treatment situations, a health care provider that has a direct treatment relationship with an individual must make a good faith effort to obtain a written acknowledgment from the individual that he or she received the provider's notice. If the provider fails to obtain the acknowledgment, it must document its good faith effort and the reason why it did not obtain the acknowledgment (e.g., "the patient refused to sign"). § 164.520. (See Wall outline, "Right to a Notice of Privacy Practices").

2. Access: Individuals have a right of access to inspect and obtain a copy their PHI. There are several circumstances in which a covered entity may deny an individual's request for access. § 164.524. (See Wall outline, "Right of Access").

3. Amendment: Individuals have a right to have a covered entity amend certain PHI about the individual that is inaccurate or incomplete. There are several circumstances in which a covered entity may deny an individual's amendment request. § 164.526. (See Wall outline, "Right to Have PHI Amended").

4. Accounting of disclosures: Individuals have a right to an accounting of certain disclosures of PHI made by a covered entity in the six years prior to the date of the individual's request. The accounting is not required to include many types of disclosures, including those for treatment, payment or health care operations. § 164.528. (See Wall outline, "Right to an Accounting of Disclosures").

5. Request additional protections (See Wall outline, "Right to Request Additional Protections").
   a. Confidential communications: Individuals have the right to request that providers and health plans make special arrangements for communicating directly with them. § 164.522(b). For example, a patient may request that a health care provider send all communications (e.g., bills, test results, etc.) to a work address rather than a home address. Providers are required to accommodate reasonable requests but may place certain conditions on the accommodation of the request.
   b. Request restrictions: Individuals have the right to request certain restrictions on the use or disclosure of their health information. § 164.522(a). For example, a patient may request that a health care provider not disclose his information for research purposes. This right is not particularly strong because it is only the right to "request" – the entity is not required to accept such requests. If, however, the entity does accept a request for a restriction, it is bound by the request (except in emergency circumstances).

D. Administrative Requirements: The privacy rule requires covered entities to comply with several administrative requirements, several of which are summarized below (See Moore outline, "Administrative Requirements").

1. Policies and procedures: A covered entity must develop and implement policies and procedures designed to comply with the privacy rule. § 164.530(i)(1). The entity must revise the policies and procedures to reflect changes in law, the privacy practices reflected in the notice, and any other policies and procedures. § 164.530(i)(2)-(5).

2. Complaints: A covered entity must provide a process for individuals to file complaints regarding the entity's policies and procedures or the entity's compliance with its policies and procedures. The privacy rule does not require the entity to act upon the complaint. The entity is only required to document all complaints filed and their disposition (if any). § 164.530(d).

3. Personnel
    a. Privacy official: A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. § 164.530(a)(1)(i).
    b. Contact person: A covered entity must designate a contact person or office who is responsible for receiving complaints and who is able to provide further information about issues addressed in the notice. § 164.530(a)(1)(ii).

4. Training: A covered entity must train all members of its workforce on the policies and procedures as necessary and appropriate for the workforce members to carry out their job responsibilities. § 164.530(b)(1). The rule provides general guidance as to when this training must be initially provided and when it should be provided after a material change in the policies and procedures. § 164.530(b)(2).

5. Sanctions: A covered entity must have and apply appropriate sanctions against workforce members who fail to comply with the entity's policies and procedures or with the privacy rule. § 164.530(e). The rule provides certain exceptions to this requirement (e.g., whistleblowers).

6. Safeguards: Covered entities must have in place appropriate administrative, technical and physical safeguards to reasonably protect PHI from any intentional or unintentional use or disclosure that is a violation of the privacy rule. § 164.530(c).

7. Documentation: The entity must maintain, in written or electronic form, a copy of the policies and procedures, a copy of any communications that the privacy rule requires to be in writing, and documentation of any action, activity or designation that the privacy rule requires to be documented. § 164.530(j).