InFocus An in-depth analysis of emerging issues in health in schools.

August 27, 2002

Safeguarding Individual Health Privacy: A Review of HIPAA Regulations

As school opens this fall, providers of health services in schools and educators have special reasons to think about protecting the privacy of the information they maintain about students. Two federal laws, one in effect for many years and the other to be complied with by April 14, 2003, make clear that students and parents must be given access to their own personally identifiable health or education files, but in general the information in those records may not be given to third parties.
The newer of the two laws, the Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996 to ensure continued health insurance coverage to persons who move from one job to another and to address the growing problem of health information confidentiality in the electronic era. Final regulations for the privacy part of HIPAA, detailing how health plans, health care clearinghouses, and health care providers must handle personally identifiable information about patients, were published in the *Federal Register* on December 28, 2000, and August 14, 2002, along with a frank acknowledgment from the agency responsible for enforcing them—the HHS Office for Civil Rights (OCR)—that many issues remain unclear and will be addressed in guidance from OCR during coming months.
The other federal law, the Family Educational Rights and Privacy Act (FERPA) is of longer standing and most schools have had some experience with it. Enacted in 1974, FERPA requires that schools that receive federal funding must hold as confidential the information in students' education records, making it available only to parents (or students at age 18) or to those within the school who have "need to know" in order to provide education. FERPA is administered and enforced by the U.S. Department of Education's Office for Civil Rights.

HIPAA and Privacy

The Health Insurance Portability and Accountability Act is a complex law and the privacy regulations issued in December 2000 and August 2002 cover only one part of its requirements. HHS has not yet issued final regs for some other parts of the law, for example, a section of HIPAA that has to do with how health information is transmitted electronically. But the privacy regulations apply so widely that they will affect most agencies and individuals involved in health care.
A little history may help to clarify the privacy regulations. When the Health Insurance Portability and Accountability Act was passed in 1996, Congress specified that if Congress did not enact health care privacy legislation by August 1999, the Secretary of Health and Human Services was to promulgate standards for the privacy of individually identifiable health information. Congress did not pass the required legislation, so HHS issued proposed privacy rules in November 1999, with a period for public comment. There were more than 52,000 comments in response to the proposal, and in December 2000 HHS issued a final "Privacy

Rule." That was just before the end of the Clinton administration, and the new Secretary of Health and Human Services, Tommy Thompson, concluded the next month that his department should review the regs, with attention to their impact on health care activities. This led to a second notice of proposed rule making, in March 2002, followed by another comment period and publication of a second final regulation on August 14, 2002, that leaves some portions of the December 2000 regulations in effect but revises others.

Among changes made in the rules this August were elimination of a requirement that patients must give consent before their personally identifiable health information may be used to provide treatment; restrictions on the use of individually identifiable patient information in the marketing of drugs and drug devices; and assurances from OCR that "incidental" disclosures of protected information that occur as a byproduct of acceptable disclosures are not a violation if the covered entity has applied reasonable safeguards to prevent them from occurring. The August 2002 rule also makes clear that parents are the representatives of their minor children and entitled to receive information about their health care, though the rule defers to state laws that may allow minors to proceed without parental knowledge in some cases, such as testing for HIV.

The Regulations

Here are some important features of the final HIPAA privacy regulations:

Covered Entities

The term "covered entities" is used throughout the privacy regulations to describe the agencies or individuals that are subject to HIPAA's privacy rules. "Covered entities" are defined to include health care plans, health care clearinghouses, and certain health care providers. For example:

- A "health plan" is any individual or group health plan that provides, or pays the cost of, medical care. Examples of health plans are employee benefit plans, health insurance issuers, health maintenance organizations, and the Medicare and Medicaid programs.
- A "health care clearinghouse" is a public or private entity that either processes or facilitates the processing of health information received from other entities.
- A "health care provider" is a provider of medical or health services such as a physician or a hospital, and "any other person or organization who furnishes, bills, or is paid for health care services in the normal course of business."
- "Health care" is defined as "care, services, or supplies related to the health of the individual," including "(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or functions of the body;" and " (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription."

Notice of Privacy Practices

The August 14 final regulations eliminate a provision in earlier regs that would have required covered entities under HIPAA to obtain consent before an individual's personally identifiable health information could be used for treatment, payment, or other health care operations. Instead, the privacy rule now allows providers to use such information without consent, but requires that the provider make a "good faith effort" to inform the individual patient about the provider's

privacy practices, preferably at the time of the first contact. Patients should acknowledge in writing that they've received this information, but the regs do not prescribe the form of the acknowledgment. HHS assures that "Failure by a covered entity to obtain an individual's acknowledgment, assuming it otherwise documented its good faith effort, would not be considered a violation of the Privacy Rule."

The regs also make clear that while prior consent to use of personally identifiable information for treatment is no longer required under HIPAA, covered entities are free to have their own consent requirements, and the privacy rule does not weaken the operation of state laws that require consent to use or disclose health information.

Minimum Necessary Disclosure

The privacy regulations generally require covered entities to make reasonable efforts to limit the disclosure of protected health information to the minimum necessary to accomplish an intended purpose, such as treating a patient or billing for service.

The regs suggest, for example, that a covered entity should identify the persons or classes of persons within the entity who need access to specific information to carry out their job duties, along with the types of protected health information they need and the conditions appropriate to such access. There may also be disclosures of protected health information to another covered entity, if the initial provider can "reasonably rely" on the other entity's need for the information for treatment, payment, or health care operations. There are some exceptions to the "minimum necessary" standard, such as uses or disclosures that are required by law.

The HHS Office for Civil Rights has promised that as the privacy regulations are implemented, it will monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the regulations don't hinder timely access to quality health care.

Incidental Disclosures

One of the points on which the Office for Civil Rights received the most comments in the interim between the December 2000 privacy regulations and the August 14, 2002, regs was whether "incidental disclosures" of protected health information would violate the rules. An incidental disclosure might occur, for example, if a third party overheard a physician discussing a patient in a hospital room or at a nursing station. Because of the concern about this issue, the OCR said in its final regulation that an incidental disclosure does not violate HIPAA if the covered entity has taken reasonable precautions to prevent it from happening.

Implications of the Regulations for School Health Services

Safeguarding Health Information

The protection of individually identifiable health information required by HIPAA extends to all forms of communication, whether oral, written, or electronic. A covered entity is expected to implement technical and physical safeguards to protect such information. For providers of health services in schools, this would seem to imply that computers containing health information, as well as written records, must be in secure locations and access to them restricted. Also, the limitations on incidental disclosure would imply that health care providers must be careful about oral communications, possibly by conducting interviews with students in secure areas—use of an open cubicle from which conversation can easily be heard might not qualify as a "reasonable safeguard" against incidental disclosure, for example.

Parental Rights

The Department of Health and Human Services has publicized the August 14

HIPAA regulations as providing parents "new rights as the personal representatives of their minor children." Generally, under the rules, parents will be able to access and control health information about their minor children. A minor is defined as an unemancipated child under the age of 18. But there are a limited number of exceptions to the general rule, including:

- Under state or other applicable laws, certain minors may obtain specified health care without parental consent—every state has a law that permits adolescents to be tested for HIV without the consent of a parent, for example. "In these exceptional cases where a minor can obtain a particular health care service without the consent of a parent under state or other applicable law, it is the minor, and not the parent, who may exercise the privacy rights afforded to individuals."
- When state law gives discretion to a health care provider to allow or deny a parent access to a minor's health information, that discretion may be exercised only by a licensed health care professional in the exercise of professional judgment.
- HHS is "neutral" about the right of a parent to health information about his or her minor child in circumstances in which the parent is technically not the personal representative of his or her minor child, particularly where state or other law is silent or unclear on this point. The regulations make no mention of whether non-custodial parents are to be considered "personal representatives" of their minor children for HIPAA purposes.

HIPAA, FERPA, School-Based Health Centers, School Nurses

The HHS Office for Civil Rights concedes that other federal laws with privacy requirements may be a problem in implementing HIPAA—for example, there are questions about how school health care providers will mesh the privacy requirements of HIPAA with the existing Family Educational Rights and Privacy Act (FERPA), which has its own privacy rules.

In a definition of the "protected health information" that is covered by HIPAA, the August 2002 final regulations specify that: "Protected health information excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act." The December 2000 final regulation noted that "individually identifiable health information of students under the age of 18 created by a nurse in a primary or secondary school that receives federal funds and that is subject to FERPA is an education record, but not protected health information."

The Office for Civil Rights commented: "While we strongly believe every individual should have the same level of privacy protection for his/her individually identifiable health information, Congress did not provide us with authority to disturb the scheme it had devised for records maintained by educational institutions and agencies under FERPA. We do not believe Congress intended to amend or preempt FERPA when it enacted HIPAA."

The December 2000 regulations make the point that an "on-site clinic" may qualify as a health care provider, and persons who work in such clinics may also qualify as health care providers. Otherwise, the HIPAA regulations are silent on school-based health centers. In practice, SBHCs sponsored by health care institutions, primarily hospitals, health departments, and community health centers, generally perceive themselves as subject to HIPAA requirements. Unless the SBHC performs school health functions or implements health mandates on behalf of the school board, the SBHC activities are assumed by the centers to be outside the scope of FERPA.

A point on which the regulations are silent is whether school nurses employed by

schools or school systems are subject to HIPAA as "health care providers." However, the 2000 regs make the apparently cautionary point that: "The educational institution or agency that employs a school nurse is subject to our regulation as a health care provider if the school nurse or the school engages in a HIPAA transaction."

This brief overview of the extensive HIPAA privacy regulations is not comprehensive, and is not intended to provide legal advice to school health care providers as to how to comply with HIPAA. We urge school health care providers to seek the advice of their state attorneys general on specific compliance issues. The Department of Health and Human Services' explanation of the final HIPAA regulations, published August 14, 2002, can be read and downloaded at
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-20554-filed
and also at these web sites:
http://www.hhs.gov/ocr/hipaa
http://www.access.gpo.gov/su_docs/aces/aces140.html