



the Policy Page

A special publication for Virginia School Boards Association's Policy Services subscribers

Number 89, March 2003
(Part 2)

WHAT TO DO WHEN THE HIPAA BEAST IS AT YOUR DOOR *

*Michael Levin and Paul Lalley, Levin Legal Group, Huntingdon Valley,
Pennsylvania, & Harlan Schreiber; New York City, New York*

**Editor's Note: This is the second part of a two-part analysis of HIPAA issues for schools. The first installment published in the December 2002 Inquiry & Analysis explained how to determine if HIPAA applies to your school district. This part analyzes various issues for those districts to which HIPAA does apply. These articles are reprinted with permission from December 2002 and January 2003, Inquiry & Analysis, as adapted from work originally appearing in December 2002 PSBA Bulletin. Copyright, 2002, Pennsylvania School Boards Association.*

If a school district concludes, after conducting a HIPAA audit, that the Privacy Rule does apply to at least one component of its operations it must resolve numerous complex implementation issues. Some of these issues are described below.

HYBRID ENTITIES

In virtually all cases where a public school entity operates a "health plan" or is a "health care provider," it should declare itself a "hybrid entity." 45 C.F.R. § 164.504. The "hybrid entity" standards under the HIPAA Privacy Rule recognize the fact that many entities have different purposes and functions. For example, hospitals are both "health care providers" and employers. When a hospital employee obtains treatment at the hospital, this might raise questions as to whether the records are employment records or health records and whether the doctor can disclose the records to the personnel director. The different functions of public school entities covered by HIPAA might likewise raise difficult questions.

Under the "hybrid entities" provision, where any individual component of an operation is either a "health plan" or a "health care provider," the entire operation will be deemed "covered" unless the entity declares itself a hybrid entity. To comply with the hybrid entity rules, a school district must both "designate" and "document" itself as a hybrid entity. 45 C.F.R. § 164.405(a). The entity, as a whole, however, must ensure that the covered component complies with the Privacy Rule. 45 C.F.R. § 164.504(c)(2). It must erect a "firewall" between the covered component and the non-covered components. 45 C.F.R. § 164.504(c)(2). The entity must make sure that all employees who work in both the covered and in the non-covered areas comply with the rules. 45 C.F.R. § 164.504(c)(2). The covered portion must comply with all of the rules governing "covered entities" pertaining to implementation policies and procedures to ensure compliance with the HIPAA Privacy Rule. 45 C.F.R. § 164.530(i).

PRIVACY OFFICIAL AND CONTACT PERSON

If deemed a "health plan" or a "health care provider," a public school entity must designate a privacy official responsible for developing and implementing privacy policies and procedures for the entity. 45 C.F.R. § 164.530(a)(1)(i). The public school entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information (PHI) and must implement policies and procedures designed to ensure compliance with the Privacy Rule. 45 C.F.R. §164.530(c)(1). The public school entity must train employees with access to PHI to follow the appropriate procedures to ensure PHI is not disclosed except as allowed by law. If the school district does not designate itself as a "hybrid entity," the training obligation may be even broader.

Complaint Procedure

The public school entity must designate a contact person or office responsible for receiving complaints under the HIPAA Privacy Rule and providing information about matters covered by the privacy notices. 45 C.F.R. §164.530(a)(1)(ii). It must also establish a process for complaints related to PHI. It must document all complaints received and their final disposition. 45 C.F.R. § 164.530(d)(1). A HIPAA-covered public school entity must sanction employees who fail to comply with the privacy policies and procedures. 45 C.F.R. § 164.530(c)(1). But it may not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual for exercising his or her HIPAA rights.

BUSINESS ASSOCIATES

Many public school entities that operate "health plans" or are covered "health care providers" contract with others to provide various services to administer the health plan or to collect fees for services. For example, third-party administrators, health care clearing-houses, auditors, and quality review organizations are just a few of the many service providers required to administer health plans or to assist health care providers. These service providers may be "business associates" under the HIPAA Privacy Rule. A "business associate" is defined as a person or entity who:

- (i) on behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this sub-chapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) any other function or activity regulated by this sub-chapter; or (ii) provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this sub-chapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from other business associate of such covered entity or arrangement, to the person.

45 C.F.R. § 160.103.

Generally, HIPAA-covered school entities must ensure their contracts with business associates contain provisions defining the permitted and required uses and disclosures of PHI by the business associate. The contract must also provide that the business associate will:

- Not use or further disclose the information other than as permitted or required by the contract or law;
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided in the contract;

- Report to the covered entity any impermissible use or disclosure of the information of which it becomes aware;
- Ensure that any agents, including a subcontractor, to whom it provides protected health information created or received from the public school entity agrees to the same restrictions and conditions that apply to the business associate;
- Make protected health information available in accordance with the HIPAA Privacy Rule;
- Make protected health information available for amendment and incorporate amendments to protected health information in accordance with HIPAA rules;
- Make available the information required to provide an accounting of disclosures;
- Make its internal practices, books and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of the public school entity available to the Secretary of Health and Human Services; and
- At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate of the public school entity.

45 C.F.R. § 164.504(e)(2)(ii)(A) through (I).

PRIVACY OF HEALTH RECORDS

TPO Exceptions to HIPAA

Originally, HIPAA's Privacy Rule stated that health records are confidential and could not be disclosed to others by covered entities with few exceptions. A covered entity was required to obtain an individual's consent prior to disclosing an individual's PHI for any reason. However, the Department of Health and Human Services modified this broad rule, so that an individual's consent is no longer necessary in order to disseminate PHI used in conjunction with "treatment, payment, and health care operations" (TPO). 45 C.F.R. § 164.506.¹ HIPAA gives some general guidelines about which TPO activities and functions are excluded from the Privacy Rule. According to the HIPAA regulations, no consent is needed to reveal PHI for: (1) the covered entity to transact its own TPO; (2) treatment activities of a health care provider; (3) payment activities of another covered entity or health care provider; (4) quality assurance activities or detection of fraud and abuse by another covered entity; (5) health care operations activities of another covered entity in a health care arrangement; and (6) the Secretary. 45 C.F.R. § 164.506(c). These guidelines provide covered entities with some clear safe havens when revealing PHI for their own TPO but suggest that they must be very careful in deciding how far to reveal PHI to other entities with which they do business. Of course, some functions the district may consider TPO may be contested by others.

Valid Authorization Necessary in Non-TPO Situations

Where the TPO exemption does not apply, a covered school district may not reveal PHI unless it has a "valid authorization" to do so. 45 C.F.R. § 164.508. A valid authorization is a document, written in plain language, containing certain "core elements:" a specific and meaningful description of the information to be used or disclosed, the names of the persons authorized to make disclosure as well as the names of the persons in the covered entity who receive the disclosure, a description of the purpose for the disclosure, an expiration date or event that relates to the purpose of disclosure, and the signature of the individual and the date of signing. 45 C.F.R. § 164.508(c)(1). In addition, the authorization must notify the individual of his right to revoke authorization and its exceptions, the ability to condition treatment, payment, enrollment or eligibility for benefits on authorization, and the potential for disclosed information to be redisclosed by the recipient and, as a result, become unprotected. The authorization may contain other provisions as long as they do not conflict with HIPAA requirements. 45 C.F.R. § 164.508(c)(2).

A covered entity may not condition treatment, payment, enrollment, or eligibility for benefits on the individual's execution of an authorization. 45 C.F.R. § 164.508(b)(4). There are three exceptions to this prohibition. First, a health care provider may require the authorization as a condition of treatment if the treatment is research-related and the individual is part of the study. Second, authorization may be required for a health

plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations. Third, authorization may be required if the provision of health care is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to this third party.

The individual may revoke authorization, at any time, but must do so in writing. 45 C.F.R. § 164.508(b)(5). However, revocation is not valid if the entity properly conditioned health care coverage on authorization or has taken action in reliance on the authorization. It is reasonable to assume that this type of revocation would become valid once the covered entity has had time to correct its actions so that it no longer detrimentally relies on the revoked authorization.

Notice of Privacy Practices

Whether or not a covered entity discloses PHI under the TPO exception or pursuant to a valid authorization, it must make a good faith attempt to obtain an individual's written acknowledgement of receipt of a Notice of Privacy Practices (NPP). The NPP must be provided by the date of disclosure unless emergencies preclude delivery until a later date. They must be written in plain language and include the following: (1) the required header; (2) a description of the types of uses and disclosures the entity may make; (3) a description of each of the purposes for which the covered entity is permitted or required to use or disclose the protected health information without the individual's written consent or authorization; (4) a statement that other uses or disclosures will be made only with the individual's written authorization and that the authorization may be revoked; (5) separate statements that the covered entity intends to engage in contacts for appointment reminders or fund raisers or if health plans, insurers or HMOs intend to make disclosures to the plan sponsor; (6) a statement of the individual's rights; (7) a statement that the covered entity is required by law to maintain the privacy of protected health information; (8) a statement that the covered entity must abide by the terms of the notice; (9) a statement that the entity reserves the right to change the terms of the notice if, in fact, the entity desires to reserve that right; (10) a statement that the individual may complain to the covered entity or to the Secretary of Health and Human Services; (11) the name or title, and telephone number of the person or office to contact for further information; and (12) the effective date. 45 C.F.R. § 164.520(b)(1).

The privacy notice must be made available on request and no later than the first day of service. Copies of the notice must be retained by the covered entity. A covered entity is prohibited from using or disclosing PHI in a manner inconsistent with its notice. The covered entity must also ensure that notice is effectively given to individuals with disabilities that may interfere with their ability to read the notice.

If the NPP is too lengthy or complicated, a "layered notice" is acceptable. A layered notice consists of a cover page with a short summary of the NPP as well as the unabridged NPP underneath. The manner of NPP delivery is somewhat flexible. Providers are not required to deliver an NPP in the same manner that it makes initial contact with a patient. For example, the NPP may be mailed to a patient even if the primary contact between provider and patient is by phone. Mailing the NPP will be considered a good faith attempt even if the individual does not return the written acknowledgement of NPP.

If a public school entity is neither a "health care provider" nor a "health care clearinghouse" under HIPAA, provides health care benefits solely through an insurance contract with a health insurance issuer or a HMO, and does not create or receive PHI other than summary health information, then the school entity is not required to maintain or provide an NPP. 45 C.F.R. § 164.520(a)(2)(iii).

Minimum Necessary Rule

Once a covered entity has determined that it may disclose PHI, HIPAA mandates that it must make reasonable efforts to limit PHI to the minimum necessary to accomplish its intended purpose. 45 C.F.R. § 164.502(b). The rule does not apply to disclosures (1) that relate to treatment by a health care provider, (2) to the

individual, (3) pursuant to a valid authorization, (4) to the Secretary, or (5) as required by law or to comply with HIPAA. This provision is intended to keep a tight lid on PHI and reduce the risk that a covered entity would use a valid authorization to reveal more PHI than needed.

STUDENT HEALTH RECORDS: COVERED BY HIPAA AND/OR FERPA?

The HIPAA Privacy Rule expressly excepts certain student records from coverage by HIPAA. Student records covered by the Family Educational Rights and Privacy Act (FERPA) are not governed by HIPAA even if they contain individually identifiable health information. Specifically, the HIPAA Privacy Rule states that: "Protected health information excludes individually identifiable health information in: (i) education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C, 1232g; and (ii) records described at 20 U.S.C. 1232g(a)(4)(B)(iv)." 45 C.F.R. §164.501.

This FERPA carve-out makes it important to understand what documents constitute "education records." Many student records do not meet FERPA'S definition of "education records." For example, "[t]he term 'education records' does not include-(i) 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." 20 U.S.C. §1232g(a)(4)(B). Therefore, 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. In that case, the notes must be used and protected in accordance with the HIPAA privacy rules. The United States Supreme Court's narrow interpretation of the term "education records" in *Owasso Ind. School Dist. V. Falvo*,² also likely decreases the FERPA exemption, leaving more student records with health information potentially subject to the HIPAA Privacy Rule.

For student records containing PHI covered by HIPAA, schools will have to use privacy notices and authorization forms. Schools will have to make available to students and parents the complaint processes required by HIPAA. Restrictions on use and disclosure will have to be honored. School employees who handle or have access to student records that contain PHI, but which are not "education records" as defined in FERPA, will have to understand the rules. These issues will have to be carefully considered when constructing the school district's policies and practices.

CONCLUSION

The implementation of HIPAA will be burdensome to all covered entities, including school districts. First, a lengthy process to determine whether and to what extent the district is covered must be undertaken. Once the determination is made, the district must then decide how to apply the Privacy Rule. This will involve adoption of new policies and procedures and creation of new infrastructure to protect PHI. Once these are established, continuing compliance with HIPAA will remain costly for the district in terms of time, money, and possible liability exposure.

¹ However, one should still check to see if state laws require consent for disclosure of PHI in some instances.

² 122 S.Ct. 934 (U.S. 2002) In *Owasso* the Court said, "FERPA requires 'a record' of access for each pupil. This single record must be kept 'with the education records.' This suggests Congress contemplated that education records would be kept in one place with a single record of access. By describing a 'school official' and 'his assistants' as the personnel responsible for the custody of the records, FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar..." 534 U.S. at 434,122 S.Ct at 940.