Protecting the privacy of medical information was primarily the responsibility of the states until Congress enacted the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This Act includes an “Administrative Simplification” provision designed to encourage the development of a standardized electronic health information system that also protects the privacy of individual health information. If Congress failed to pass health information privacy legislation within three years, HIPAA directed the Secretary of Health and Human Services (HHS) to issue privacy regulations. Congress did not pass the legislation, so following a lengthy process, HHS published the final HIPAA Privacy Rule on August 14, 2002³. The Privacy Rule establishes a national minimum standard of privacy applicable to health plans, certain health care providers, and health care clearinghouses. Except for “small health plans,”⁴ which must comply by April 14, 2004, the deadline for compliance is April 14, 2003.

The Privacy Rule is one of three regulations required by HIPAA. The other two are regulations governing the security of electronic health information and standards for electronic transactions. Unless a one year extension was requested, the effective date for the regulations on “Electronic Standards and Code Sets” was October 15, 2002. Proposed security regulations were published in 1998, but as of December 26, 2002, final regulations have not been published.

The purpose of this paper is to inform members of the National Association of Independent Schools (NAIS) about the Privacy Rule and how its key provisions may or
may not affect member schools. The Rule is most likely to affect private, independent schools directly when they are providers of health care or have self-insured health plans, health flexible spending account plans, or employee assistance programs. At the end of this publication is a hypothetical to help illustrate how HIPAA may impact an independent school.

Who is covered by the Privacy Rule?5

The HIPAA Privacy Rule applies to health plans, health care clearinghouses, and health care providers who transmit6 personal health information in electronic form in connection with specified financial and administrative activities related to health care, such as processing insurance claims.7 Persons or legal entities to whom the Rule applies are described as “covered entities.”

Health Plans.8 A “health plan” is “an individual or group plan that provides, or pays the cost of, health care.” The term is defined broadly enough to include most employer-sponsored health plans, including medical plans, stand-alone dental and vision plans, employee assistance plans (EAP) and health flexible spending account plans.9 However, health plans with fewer than 50 participants and self-administered by the employer are not subject to the Privacy Rule. Also, accident and life insurance, disability income coverage and workers’ compensation benefits10 are not covered by the Rule. Health information held in employment records by an employer is also not covered.11

An employer, as sponsor of a health plan, is not regulated by the Rule, but many of the requirements may be applied indirectly through contract and plan document provisions required under the Rule.12 Where the employer is both the plan sponsor and the plan administrator, as may be the case in self-insured plans, the employer, as administrator, will be responsible for assuring plan compliance with HIPAA. While most NAIS-member schools may not administer their own group health insurance plans, they may administer other covered employee benefits such as health flexible spending accounts. If so, and the plan has more than 50 participants, the school should prepare an implementation plan to assure compliance with the Privacy Rule to meet requirements such as amending plan documents, providing appropriate notices to plan participants, and erecting

---

5 45 C.F.R. §160.102.
6 The provider’s coverage by the Rule is based upon electronic transmission, rather than electronic receipt, of the health information.
7 45 C.F.R. §160.103. See, in particular, the definitions of group health plan, health care, health care provider, health plan, and transaction.
8 45 C.F.R. §160.103. See the definitions of group health plan and health plan.
9 The HHS Center for Medicare and Medicaid Services is reported to be reviewing whether health flexible spending accounts should be included.
10 45 C.F.R. §164.512(l).
11 45 C.F.R. §164.501. See the definition of protected health information. Employment records are excluded from the definition.
12 45 C.F.R. §164.504(f)(1).
adequate firewalls around employees handling protected health information in connection with the plan. Schools that have direct involvement with the administration of the health plan (i.e., certain school employees handle and/or are involved in specific health related questions or administrations), even when they act primarily as sponsors of the plan, should work with both the insurance company and school legal counsel to ensure that the school either does not fall under HIPAA or has appropriate safeguards in place.

*Helpful Hint:* Some schools may find that the only triggering activity they participate in is providing health flexible spending accounts. Schools may wish to look into contracting with an outside company to provide complete services in this area so that the school is not actually administering the plan.

**Health Care Clearinghouses.** One of the covered functions that independent schools are not likely to be involved in is clearinghouse activities. A health care clearinghouse is an entity that is involved in the processing of health information into or out of a standard format. For example, a health care provider might use a billing service that translates the provider’s data from a nonstandard into a standard format for submitting claims to a health insurance plan.

**Health Care Providers.** A school that provides health care services to students or employees and that transmits health information electronically in a standard format in connection with a HIPAA transaction may be subject to the Privacy Rule as a “covered entity.”

A “health care provider” is a “person or organization who furnishes, bills, or is paid for health care in the normal course of business.” In reviewing their activities to determine if they are providing “health care,” schools must consider the broad definition of the term in the regulation. The definition includes services and supplies, encompassing far more than traditional medical services. For example it includes rehabilitation, assessment, counseling, and medical equipment, among other things. Schools should have counsel review their health care-related activities in light of this broad definition. If the school provides employee health services, student counseling, or health services, including a school nurse, it may be a “provider.”

If a school is providing health care, it must then examine whether there is any electronic

---

13 45 C.F.R. §160.103. See the definition of *health care clearinghouse.*
14 45 C.F.R. §164.501. See the definition of *protected health information*.
If the school is subject to the Family Educational Rights and Privacy Act of 1974, as amended, (FERPA or the “Buckley Amendment”), its student health records on students will not be considered “protected health information” even though the school may be a “health care provider.”
15 45 C.F.R. §160.103. See the definition of *health care provider.*
16 45 C.F.R. §160.103. See the definition of *health care.*
transmission of health information in connection with a HIPAA transaction,\textsuperscript{17} which generally involves electronic transmission of personal health information for health insurance related purposes.\textsuperscript{18} Electronic transmission covers most types of electronic communication except telephone voice transmissions and paper-to-paper faxes.\textsuperscript{19} For example, if the school has an on-site nurse, but it does not bill for services and does not transmit health information electronically in a "HIPAA transaction," the school would be a provider but not a "covered entity." At the time of this article, HIPAA transactions are defined as including the following 11 types of transmissions.\textsuperscript{20}

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. Enrollment and disenrollment in a health plan.
6. Eligibility for a health plan.
7. Health plan premium payments.
8. Referral certification and authorization.
10. Health claims attachments.
11. Other transactions that the Secretary may prescribe by regulation.

All of the transactions described are related to transmissions for billing and health insurance purposes, particularly where transmission is, or will be required in the future to be, in a standard format as health insurance companies generally require. Use of a third party to handle the transmission does not prevent the health care provider from becoming a covered entity. Unless done for one of the enumerated purposes above, internal transmissions would not make the school a covered entity.

\textit{Helpful Hint:} Schools only fall into this category if they are a health care provider \textit{and} they transmit the information electronically. Schools should look at what they do with health information and if any electronic transmission of the health information is necessary.

\textit{Helpful Hint:} Transmission of the student injury information should be to another health care provider or to the parents. Transmitting the information to the parents' health insurer could raise concerns since it might be interpreted as being transmitted electronically in connection with a health insurance claim.

Once a health care provider qualify as a “covered entity,” however, all of its health information is subject to the Privacy Rule, regardless of how it is recorded or maintained.

\textsuperscript{17} HHS has implied in some of its published comments that the electronic transmissions are covered only if in standard format, but this is a nuance that should be evaluated by counsel.

\textsuperscript{18} 45 C.F.R. §160.103. See the definition of \textit{transaction}. Eleven types of transmission of health information are described.


\textsuperscript{20} 45 C.F.R. §160.103
For example, once the entity is covered by the Privacy Rule, the Rule applies to its paper, as well as its electronic, health records.

**What about receiving electronic information from parents or others?**
HIPAA requires that the health care provider transmit the information. Therefore, if parents or others are electronically sending the school health information the transmission should not trigger HIPAA for the school. In other words, schools that ask parents to electronically transmit basic information related to allergies or recurring conditions to the school’s nurse do not trigger HIPAA by receipt of this information alone.

**What are the administrative requirements for a covered entity?**

If your school falls into one of the above described categories, it is a covered entity under HIPAA. Covered schools must adopt privacy policies and procedures and give written notice of their privacy practices. It is important for schools to reserve in their policies the right to change privacy practices. For health plans, notice must be given at the time of enrollment and every three years thereafter. Health care providers have to give notice at the time service is first delivered, ask for a written acknowledgment of the notice, post the notice on the premises, and make details of the privacy practices available to individuals upon request. Whenever the practices change, the notice has to be updated.\(^{21}\)

Covered schools will also be required to:

- Adopt administrative, technical, and physical measures to protect the privacy of protected health information. This is in addition to any requirements for the security of electronic information.\(^{22}\)

- Appoint a privacy officer who is responsible for development and implementation of privacy policies and procedures.\(^{23}\)

- Train members of the workforce about the privacy policies and procedures.\(^{24}\)

- Set up a system for accounting for disclosures of protected health information for the past six years.\(^{25}\) The accounting does not cover disclosures under an authorization signed by the individual (including parent, guardian, or other personal representative). There are other exceptions of limited applicability with regard to schools.

---

\(^{21}\) 45 C.F.R. §164.500 and §164.520.  
\(^{22}\) 45 C.F.R. §164.530(c).  
\(^{23}\) 45 C.F.R. §164.530(a).  
\(^{24}\) 45 C.F.R. §164.530(b).  
\(^{25}\) 45 C.F.R. §164.528
Where a school has a health plan or limited health care provider activities in addition to other non-covered functions, it has the option of declaring itself to be a “hybrid entity” and designating the covered functions that will be included in the health care component. In this way, the school can limit the implementation of the HIPAA Privacy Rule to the health care component. For example, only those employees in the health care component would have to be trained. Once this designation occurs, however, the health care component is treated as if it were a separate legal entity with regard to the use and disclosure of protected health care information. The health care component cannot disclose information to the non-health care components without the authorization of the individual or as permitted by the Rule. For this reason, it is important to include in the health care component those service areas that would need access to protected health information.\(^\text{26}\)

*Helpful Hint:* Schools with more robust health care provisions, those with larger infirmaries and substantial counseling services may want to look closely at the hybrid option. Schools interested in pursuing the option of becoming a “hybrid entity” should consider all of the overlapping areas that may need access to the health information (e.g., counseling, school nurse, any physicians on staff, etc.). Those within this entity will be responsible for the health information and its protection. Schools should consult with counsel if they are interested in going down this road.

**What health information is protected by the Privacy Rule?\(^\text{27}\)**

HIPAA designates individually identifiable health information created or received by a covered entity as “protected health information.” (PHI). Most people think of “health information” as that information contained in a hospital-or physician-created medical record. “Health information” is defined much more broadly by the Privacy Rule, however. The definition includes “any information, whether oral or recorded in any form or medium.” It covers any information related to the “past, present, or future physical or mental health or condition of an individual,” as well as information about an individual’s care and payment for care.

Health information is considered “individually identifiable” whenever it actually identifies the individual or there is “a reasonable basis to believe the information can be used to identify the individual.” It includes demographic information collected about a person. This means that if a covered entity disclosed health information about a person and there was anything contained in that disclosure that could reasonably be used to identify that person, even though no name is included, the entity would be in violation of the Privacy Rule.

The Rule establishes a class of information that may be disclosed without being subject to the requirements of the Rule. This information is described as “de-identified,” but to

\(^\text{26}\) 45 C.F.R. §164.504(a) – (c).

\(^\text{27}\) 45 C.F.R. §160.103. See the definitions of *health information* and *personally identifiable health information.*
qualify for this exception, 18 specific kinds of identifiers have to be removed. \(^{28}\) For example, references to geographic locations smaller than a state could not be included. \(^{29}\)

If a school is covered by the Family Educational Rights and Privacy Act of 1974, as amended (FERPA or the “Buckley Amendment”), personally identifiable health information on students is excluded from the definition of protected health information. The Privacy rule defers to the privacy protections provided by FERPA. \(^{30}\) Those schools that do not receive funds from the United States Department of Education and are therefore not subject to FERPA, however, must apply the HIPAA Privacy Rule to their student health records if the school qualifies as a “covered entity.”

**How may protected health information be used and disclosed?**

The Privacy Rule distinguishes between “use” and “disclosure” of protected health information. “Use” generally applies to how protected health information is used within the covered entity, while “disclosure” usually applies when information is shared outside the entity. \(^{31}\) Using or disclosing the minimum information necessary to achieve the purpose of the use or disclosure is sometimes required and always encouraged. \(^{32}\)

If a school is a covered entity, it may use or disclose protected health information only as permitted or required by the regulation. Some uses or disclosures are allowed without the individual’s authorization; some are allowed if the individual has an opportunity to object; and others are permitted only with the individual’s written authorization. A brief description of the permitted and required uses delineated in the regulations is below. Except when disclosing information to the individual (or a personal representative) or to HHS, a covered entity is not required by the Rule to disclose health information. While the Privacy Rule may not require disclosure, however, other laws may. For example, if a court orders the release of protected health information, the entity could not use the discretion granted under the Privacy Rule to refuse to comply with the order.

Protected health information may be used or disclosed when an individual has provided written authorization that complies with the Rule. An authorization can be revoked in writing, except to the extent the covered entity has already acted in reliance upon it. Generally, services may not be conditioned upon a person signing an authorization, but treatment related to academic research may be conditioned upon the signing of an authorization for access to the protected health information related to the research project. Also, enrollment in a health plan or payment of benefits can be conditioned upon receiving an authorization for access to protected health information. In each exception, access to the information is an integral part of the service provided.

---

\(^{28}\) 45 C.F.R. §164.514(a) - (c).

\(^{29}\) Not discussed here is another category of health information that can be disclosed for academic research purposes under some circumstances. See 45 C.F.R. §164.514(e) for a definition of limited data set.

\(^{30}\) 45 C.F.R. §164.501. The definition of protected health information excludes records covered by FERPA.

\(^{31}\) 45 C.F.R. §164.501. See the definitions of disclosure and use.

\(^{32}\) 45 C.F.R. §164.502(b)
Incidental uses and disclosures are permitted as long as they are reasonable. For example, if a school administrator takes reasonable precautions when discussing protected health information, but a third party overhears it, the administrator will not be deemed to have violated the Privacy Rule.

Also of interest to schools are several other allowed uses and disclosures not requiring written authorization: facility (usually hospitals) directories; next of kin involved in care; marketing; fund raising; averting a serious threat to health or safety; health oversight activities; judicial and administrative proceedings; law enforcement; public health activities; research; cases of abuse, neglect, or domestic violence; and workers compensation. While all of these areas require analysis if a school is a covered health care provider, it is particularly important to pay attention to disclosures related to law enforcement and judicial and administrative proceedings. Schools that are covered should have in place a procedure for dealing with law enforcement requests for access to health records and should consult with counsel whenever health records are subpoenaed.

A school that qualifies as a health care provider will be concerned with uses and disclosures related to treatment, payment, and health care operations. These are allowed without specific patient authorization. For example, a school providing medical treatment to students does not have to get student permission to share information with its employees involved in treatment. Likewise, the school can use the information for quality assurance or for billing purposes.

Finally, if a school hires a contractor to perform services requiring access to protected health information, the school must require the contractor to execute a “business associate agreement” under which the contractor agrees to protect the privacy of the information. The Rule does not apply to the contractor, but HHS will expect the school to enforce the contract provisions, or notify HHS if unable to do so and it is impractical to cancel the contract. Legal and accounting services are examples of business associate activities.

33 45 C.F.R. §164.510(a); §164.510(b)
34 45 C.F.R §164.10(a).
35 45 C.F.R. §164.501 and §164.508(a)(3)
36 45 C.F.R. §164.150(b) ; §164.514 (f) and § 165.522.
37 45 C.F.R. §164.512(j).
38 45 C.F.R. §164.512(c). (d).
39 45 C.F.R. §164.512(c).
40 45 C.F.R. §164.512(f).
41 45 C.F.R..§164.512(b) and §512(e).
42 45 C.F.R. §164.512(i) and §164.514(e).
43 45 C.F.R. §164.512(c).
44 45 C.F.R. §164.512(l).
45 45 C.F.R §164.502(e); §164.504(e); and §164.532(d) and (e). Business associate is defined in 45 C.F.R.§160.103.

© 2003 National Association of Independent Schools
What are the rights of the person who is the subject of personally identifiable health information?:

The Privacy Rule grants individuals (or their personal representatives) the right to see and copy their health information, with some exceptions. If a covered entity denies an individual access, the entity must have a process for review of that decision, with a few exceptions, such as access to psychotherapy notes. For example, if an individual’s health information refers to another person and a health care professional believes access might be harmful to the other person, access could be denied but the individual would have to be advised of his or her rights to review of that decision. Review must be by a licensed health care professional who was not involved in the decision to deny access.

Individuals have the right to request that a covered entity amend their health information if they believe the contents to be in error, but the entity has the right to refuse to do so, especially if it believes the information to be accurate. The individual does have the right to place his or her own statement about the accuracy of the information into the record.

Another important right is the right to an accounting of most disclosures of protected health information for six years. Individuals have the right to know to whom their health information has been disclosed, unless they have authorized the disclosure in writing or the Rule otherwise exempts a disclosure from the accounting requirement.

Helpful Hint: Schools should look at how they will implement these requirements on a practical level and inform parents and students of these procedures before issues arise.

Who may exercise privacy rights on behalf of minors?:

Generally, it is the parents or guardian rather than the minor who may exercise rights under state law with regard to the minor’s health information. This means that a school would obtain authorization from a parent, for example, before disclosing a student’s health information to a third party. Sometimes, however, state law gives a minor the right to exercise control over his or her medical care, so the Privacy Rule recognizes this same right with regard to related health information. Also, parents sometimes agree to confidentiality between the minor and a health care provider, and if they do, the Privacy Rule allows the minor to exercise rights with regard to access and disclosure.

Helpful Hint: The issue of confidentiality between a minor and a health care provider is a substantial one, particularly with regard to student counseling and the issues it may raise. Schools should craft a policy and ensure that the proper forms are signed as required to implement the policy effectively.

---

46 45 C.F.R. §164.524. This section details the right of access and what the covered entity must do if access is denied.
47 See 45 C.F.R. §164.526 for details.
48 45 C.F.R. §164.502(g).
A covered entity may refuse to disclose protected health information to a parent or guardian (or other personal representative) of a minor where abuse or neglect by that person is involved, particularly where disclosure could endanger the minor. The decision about whether it is in the minor’s best interest to disclose protected health information to the personal representative should be made by a licensed health care professional.

*Helpful Hint:* Schools may want to identify someone within the community who will make this decision before the issue arises.

In some instances, boarding school administrators, acting *in loco parentis*, may be considered the personal representative of a student with regard to obtaining protected health information on the student from a local hospital or other health care provider. In this role, the school may be in the position of exercising the minor student’s HIPAA rights.

*Helpful Hint:* Boarding schools in particular may want to receive guidance from counsel on this issue to determine if the boarding school administrators have such rights in that school’s case. This will be very important, particularly if the school has designated itself as a hybrid entity as discussed on page five of this article.

**How is the Privacy Rule enforced?**

Anyone who believes that a covered entity is not complying with HIPAA can file a complaint with the Secretary of HHS (the Office of Civil Rights will handle enforcement). It does not have to be the person whose privacy rights have been violated. The complainant could be an interested person or organization. HHS is responsible for investigating complaints and is authorized to impose civil monetary penalties. Criminal prosecution is possible for intentional disclosures in violation of HIPAA, especially if done for profit.

**Are state privacy laws preempted by HIPAA?**

HIPAA preempts only those state laws that are less stringent than HIPAA. In other words, if state law gives individuals more privacy protection than the Privacy Rule does, the state law governs. Most states have numerous laws affecting the privacy of health information and those laws vary widely. Coordinating these laws with HIPAA will be extremely complex.

**Conclusion**

Each member of NAIS should take the time to evaluate its activities to determine if it is involved in any functions covered by HIPAA so that an implementation plan can be developed before the April 14, 2003 implementation deadline. Smaller institutions with

49 45 C.F.R. §164.306.
50 45 C.F.R. §160.201- §205.

© 2003 National Association of Independent Schools
small health plans may have even longer if the only covered function is a group health plan with less than five million dollars in receipts. Schools are strongly encouraged to work with counsel to ensure that their plans meet the HIPAA requirements and the schools’ options under these new regulations are protected.
The following hypothetical is presented as an example of how the HIPAA Privacy Rule might affect a private independent school.

**HYPOTHETICAL**

Green Day School has 75 employees. Sixty employees participate in a health flexible spending account plan; 55 have a dependent flexible spending account; and 51 participate in the health insurance plan for which Green Day pays 75 percent of the premium. The headmaster does not think that the flexible spending accounts are health plans under HIPAA since they are just accounts where Green Day holds the employee’s money and pays it out to the employee when detailed receipts for qualified services are submitted. Since the school is not administering its own group health plan, the headmaster does not believe the school will have to be concerned with HIPAA Privacy Rule requirements with regard to the plan.

Does the HIPAA Privacy rule apply to any of these plans? If so, how is Green Day affected and what should the headmaster do?

**Health flexible spending account plan.** Green Day should treat the health flexible spending account plan as a “health plan” under the Privacy Rule, although CMS (Centers for Medicare and Medicaid Services in the Department of Health and Human Services) is rumored to be re-evaluating whether such a plan is really a health plan under the Rule. Even though the flexible spending account is returning to the employees money they have contributed, it is still a plan that Green Day administers, that pays for the cost of health care, and that has more than 50 participants. These are the components that qualify a plan as a “health plan” under the rule.

Since the health flexible spending account plan will have annual receipts for the 60 employees of less than five million dollars, it is a ‘small health plan” and Green Day will have until April 14, 2004 to implement the Privacy Rule requirements for the plan. Implementation may include declaring Green Day to be a “hybrid entity” and the plan to be the “health care component.” This means that if Green Day has no other covered function, it will only apply the Rule’s requirements to this one designated area. However, Green Day must be careful not to disclose an employee’s protected health information to anyone outside the health care component, unless authorized by the employee or otherwise permitted by the Rule or required by law.

**Dependent flexible spending account.** Since it does not provide or pay for health care, the dependent flexible spending account is not a health plan under the Privacy Rule. These accounts simply reimburse the employee for qualifying dependent care expenses.

**Health insurance.** The Green Day employee group health insurance plan is a covered entity under the Privacy Rule. It would be exempt from the Rule only if it had less than 50 participants and was self-administered. Since the plan is commercially insured, the insurer will be responsible for assuring that the plan complies with the Rule requirements.
Green Day, as the sponsor of the plan, is not the covered entity. However, Green Day will be affected by the Rule since the plan may not disclose protected health information to the plan sponsor without amending the plan documents to assure that the sponsor is restricted from using or disclosing that information except as permitted by the Privacy Rule or otherwise required by law. Without amending the plan documents, Green Day may receive summary information about claims whenever it needs data for obtaining premium quotes or for modifying or terminating the plan, and may receive information on whether individual employees are enrolled in the plan. Green Day may also receive health information from employees who ask Green Day to serve as an advocate with the insurer, but getting too involved in advocacy for employees could raise issues about whether Green Day is receiving protected health information from the insurer or is partially self-administering the plan.

*N.B. The information herein should not be considered legal advice. School administrators should consult school counsel who can evaluate each school’s circumstances and offer advice on how the Privacy Rule may or may not apply.*