HIPAA Privacy Rule Primer

for the College or University Administrator

On August 14, 2002, the Department of Health and Human Services ("HHS") issued final medical privacy regulations (the "Privacy Rule") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[1] which must be implemented by April 14, 2003. The Privacy Rule applies only to health plans, health care clearinghouses and health care providers ("covered entities"). Many colleges and universities ("Colleges") will be affected through their health plans and some of their health care provider activities.

PURPOSE OF THE PRIVACY RULE

Before HIPAA, no national standard existed for the protection of a person's medical information. With the adoption of the HIPAA Privacy Rule, a minimum level ("floor") of protection was created nationwide. Rather than apply the usual federal preemption doctrine, however, HIPAA allows the application of more stringent state laws[2] and requires the coordination of HIPAA with other federal privacy laws, except the Family Educational Rights and Privacy Act, which continues to control with regard to student records.

Now, individuals are assured of access to their medical information and are provided substantial protection regarding its use and disclosure, including an accounting for most disclosures for six years.[3] Use or disclosure of the minimum information necessary to achieve the purpose is sometimes required and always encouraged.[4]

ENTITIES COVERED BY THE PRIVACY RULE

The Privacy Rule applies to health plans, health care clearinghouses, and health care providers.[5] Health care clearinghouses, which process or facilitate the processing of health information between or among other entities, are not discussed here since it would be unusual for a College to be acting in this role. The provisions on health plans or health care providers may affect Colleges, however.

[1] The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 110 Statutes 1936 (August 21, 1996), commonly known as "HIPAA."

[2] 45 C.F.R §§160.201 – 205. Coordinating the requirements of the Privacy Rule with more stringent state laws is somewhat complex. The identification of state laws affecting the privacy of medical information is no small task; determining how the state laws are coordinated with HIPAA is equally difficult. In some instances, the governor of a state may submit a request to the Secretary of HHS to allow less restrictive state laws to control if the laws meet certain requirements, such as they are necessary to prevent health care fraud and abuse.

[3] 45 C.F.R. §164.524. This section establishes the right to access and to a copy of one's medical information. In come limited circumstances, access can be denied or, in the case of certain research projects involving treatment, temporarily suspended. The Rule provides for reviewable and non-reviewable grounds for denial. For reviewable grounds, the Rule defines a an appeal process for challenging the decision.

[4] See 45 C.F.R. § 164.514(d)(1). The objective is to encourage the use or disclosure of the least amount of PHI, while not encroaching upon the judgment of health care professionals regarding how much information they may need in treating the patient.

[5] See 45 C.F.R. § 160.103 Definitions.

* Prepared by Gerald W. Woods, Kilpatrick Stockton LLP, Augusta, GA. December 2002.

HEALTH PLANS

The definition of "health plan" is broad enough to include most employer-sponsored health plans.[6] The term covers medical plans, stand-alone dental and vision plans, employee assistance programs ("EAP") and medical flexible spending account plans, but not plans with less than 50 participants and that are self-administered by the employer and not workers' compensation, disability income coverage or accident only coverage.

A health plan would be the covered entity, not the College as plan sponsor/employer or the plan's third-party administrator (TPA).[7] However, health plan documents must include provisions that limit the protected health information the sponsor receives, and the plan contract with the TPA must require the handling of information in accordance with the Privacy Rule. The TPA and plan attorneys, accountants, consultants, etc. are considered "business associates" of the plan. This means that the plan (or the College acting on behalf of the plan) must have agreements with the TPA and other business associates that include provisions requiring adherence to the Privacy Rule requirements.

Sometimes the College will be both the plan sponsor and the plan administrator. This situation requires the College to have access to PHI to carry out its duties. Recognizing this possibility, the Rule allows disclosure of PHI to the sponsor to fulfill this role if the plan document is amended to include provisions governing the sponsor/employer receipt and use of PHI. First, the plan document (i) has to describe the permitted uses and disclosures with regard to the sponsor, (ii) has to make clear which employees of the sponsor will be given access to the PHI to carry our plan administration duties, and (iii) has to provide a process for resolving issues of non-compliance with the Privacy Rule by anyone given access to PHI.[8]

Second, the plan documents must require the sponsor/employer to certify to the plan they will not use or disclose PHI, except as required by law or permitted by the plan document. The sponsor also has to certify that it will impose these requirements on its subcontractors or agents that have access to PHI.

Third, the plan document has to be amended by the sponsor to create firewalls between the employees handling PHI in carrying out plan administration duties and other employees of the sponsor. For example, the sponsor may not use the PHI for employment-related purposes.[9]

If the plan is insured and the College is not maintaining or receiving protected health information, the insurer would be responsible for complying with the Privacy Rule requirements. The College would not have to amend the plan documents or provide certifications mentioned above. The insurer could disclose summary information to the College, as health plan sponsor, for insurance premium bid purposes or for changing the plan and in notifying the sponsor whether a person is participating in the plan[10].

The deadline for health plan compliance is April 14, 2003, except "small" health plans have until April 14, 2004.[11] "Small" health plans are those with annual receipts of $5 million or less.[12]

---

[6] 45 C.F.R. §164.501. Definitions. *Group health plan* and h*ealth plan.* Public Colleges should consult with counsel about their state's position on whether the definition of "health plan" includes state government plans. Some attorneys have expressed doubt about its application.

[7] 45 C.F.R. §160.103 Definitions. A *Covered entity* is a health plan, health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

[8] 45 C.F.R. §164.501(f)(1).

[9] See 45 C.F.R. § 164.504(f)(2) for other details of what the plan sponsor must agree to do.

[10] 45 C.F.R. § 164.504(f)(3)

[11] 45 C.F.R. §164.534(b).

[12] 45 C.F.R. §160.103 Definitions.

HEALTH CARE PROVIDER

Except for academic medical centers, most Colleges do not think of themselves as health care providers. However, if they provide any "care, services, or supplies related to the health of an individual" they may qualify as "health care providers" under the Privacy Rule. For example, counseling, physical assessments, or providing medical devices or equipment will qualify. [13]

A health care provider becomes a covered entity only if it transmits health information in electronic form in connection with a "HIPAA transaction."[14] A "HIPAA transaction" is the electronic transmission of information "to carry out financial or administrative activities related to health care." The types of transmissions constituting a HIPAA transaction include:

- "Health care claims or equivalent encounter information.
- Health care payment and remittance advice.
- Coordination of benefits.
- Health care claims status.
- Enrollment and disenrollment in a health plan.
- Eligibility for a health plan.
- Health plan premium payments.
- Referral certification and authorization.
- First report of injury.
- Health claims attachments.
- Other transactions that the Secretary [of HHS] may prescribe by regulation."[15]

Electronic transmission is a required element for a health care provider to be considered a "covered entity," but once a provider becomes a covered entity, all of its PHI is subject to the Rule. The covered entity's written records and oral communications, as well as its electronic ones, become subject to the Rule's requirements. The one exception, important to Colleges, is student health information subject to the Family Educational Rights and Privacy Act (FERPA)."[16]

Individually identifiable health information about students is not considered "protected health information" if it is either an education record under FERPA or is exempted from FERPA. Student health information exempt from FERPA may be used only for providing care to the student and may not be disclosed otherwise, except to a health care professional designated by the student. If the College violates the FERPA exemption, the student health record becomes an education record governed by FERPA.

Most Colleges will have only a few activities qualifying as "covered functions"[17] under the Privacy Rule. In that event, the College may declare itself to be a "hybrid entity"[18] and designate a health care component or components that will contain the covered functions. Only the health care component is then subject to the Rule, but disclosure of protected health information to the non-health care component is treated the same as disclosure to a separate legal entity. For example, if a College's only covered function is its counseling center, the College may declare itself a hybrid entity, designate the center as its health care component and ensure that the health care component complies with the Rule.

---

[13] See 45 C.F.R. §160.103 Definitions. The definition of *health care* includes other helpful examples. See, also, the broad definition of *health care provider*.
[14] 45 C.F.R. §160.103 Definitions. *Covered entity.*
[15] 45 C.F.R. §160.103 Definitions. *Transactions.*
[16] 45 C.F.R. §164.501 Definitions. *Protected health information.* The definition of *protected health information* excludes education records covered by the Family Educational Rights and Privacy Act (20 U.S.C. §1232g and certain student records exempted from the Act (20 U.S.C. §122g(a)(4)(B)(iv)).
[17] 45 C.F.R. §164.501 Definitions. *Covered functions.*
[18] 45 C.F.R. §164.504(a) - (c).

Health information in employment records held by the College in its role as an employer is not protected health information. For example, even though an academic medical center is a covered entity, health information in its personnel records will not be considered protected health information.

USE OR DISCLOSURE[19]

The Privacy Rule prohibits uses and disclosures of PHI unless permitted or required by the Rule.

Protected health information may be disclosed to the person who is the subject of the information without requiring the individual to sign an authorization. This means that a physician, for example, may communicate freely to a patient about his or her own protected health information. This would allow an academic medical center physician to speak to his or her patient about participating in a clinical study, but a physician/researcher could not go to various hospitals to review the medical records of patients and use that information to recruit clinical study participants.

A health care provider may use or disclose PHI for treatment, payment, or health care operations purposes. For example, a College student health service treating non-students and engaging in a "HIPAA transaction" as described above will be a covered entity and the health care information on these non-student patients will be protected health information. However, the student health service can use the individual's health information in treating the patients, communicating with insurers for payment, and for health care operations such as quality assurance or complying with accreditation requirements. Written policies and procedures governing the use and disclosure of the information are required, and patients are entitled to notice of the institution's privacy practices.[20]

A covered entity may disclose health information to its "business associates" who sign "business associate agreements" with the entity. A business associate is an entity or a person, other than a member of the workforce, who provides services for or on behalf of a covered entity. For example, a covered entity's attorneys, accountants, and consultants who need access to individual health information to perform their services would be business associates.[21]

In some instances, PHI may be disclosed if the person has the opportunity to agree or object to the disclosure. Also, disclosure is permitted for health plan underwriting purposes, for certain fundraising uses, and if the information qualifies as a "limited data set."

If an individual requests his or her PHI, disclosure is required. Also, the Secretary of HHS may require disclosure.

WRITTEN AUTHORIZATION FOR USE OR DISCLOSURE

A person who is the subject of the protected health information may execute a written authorization for its use or disclosure.[22] The written authorization must be in the form specified by the Rule and may not be combined with any other document, except one related to research may be combined with any other written permission for the

[19] 45 C.F.R. §164.502. This section explains the general rules about permitted and required uses and disclosures .
[20] 45 C.F.R. §164.530(i).
[21] 45 C.F.R. §164.103 Definitions. *Business associate***.** Counsel for some hospitals where Colleges send students for clinical training have expressed the intent to require Colleges to sign "business associate" agreements to cover the students with regard to removal of PHI from the facility for use in their classes or in preparing papers. Other hospital attorneys have stated that they do not think the business associate agreement applicable to students in training, but they may apply the concept to College faculty who come to the hospital to serve as preceptors for the students. Still others have acknowledged that neither approach may be technically correct, so they intend to limit the amount of personally identifiable data a student may remove. Some of the latter attorneys have admitted that it may be difficult to remove enough information to meet the HIPAA Privacy Rule requirements for "de-identified" data. De-identified data is not considered to be PHI because so many identifiers have been removed.
[22] 45 C.F.R. §164.508(a)(1). Although the Rule grants an individual the right to a copy of his or her protected health information, the Rule does not require a covered entity to disclose information to a third party in response to a written authorization.

same study. It may be revoked in writing except to the extent action has been taken in reliance upon it. If a covered entity is obtaining the authorization, the entity must provide the individual a copy.

Covered entities are prohibited from conditioning their treatment, payment and service decisions on obtaining a written authorization from an individual for some other use or disclosure of the person's protected health information. Some exceptions to this provision are recognized, however. A provider may condition research related treatment on obtaining an authorization for the use or disclosure of PHI for the research project, since the treatment is an important part of participating in the research. A health plan may condition enrollment or eligibility for benefits on obtaining an authorization for disclosure of health information (excluding psychotherapy notes) necessary for eligibility or underwriting decisions. If a provider is asked to create protected health information for disclosure to a third party, the provider may condition the provision of the related health care on obtaining an authorization for disclosure to that party.

A valid authorization will be in writing and contain "core elements," including: (i) a specific and meaningful description of the information to be used or disclosed; (ii) the identity of the person authorized to disclose the information; (iii) the identity of the person to whom it is to be disclosed; (iv) the purpose of the requested use or disclosure ("at the request of the individual" is sufficient); (v) an expiration date or event related to the individual or the purpose of the use or disclosure ("end of research study" or "none" is sufficient for use or disclosure for research); and (vi) the signature of the person or their personal representative and the date. It must also contain certain "required statements" such as those related to (i) an individual's right to revoke; (ii) the ability or inability to condition treatment, payment, enrollment or eligibility for benefits; and (iii) the potential for the PHI, once disclosed, to be re-disclosed outside the protection of the Privacy Rule.[23]

In limited circumstances, an Institutional Review Board (IRB) or a special privacy board may approve waivers or modifications of the written authorization for research purposes. The IRB is the same one Colleges use for reviewing research involving human subjects. Now, the IRB will have additional duties under HIPAA, unless the College chooses to appoint a special privacy board to handle the HIPAA responsibilities. For HIPAA purposes, the IRB or privacy board may review waiver requests involving covered entities other than the College, as well as College related ones. Of course, these other entities may choose to require review by their own IRB or privacy board.[24]

USE OR DISCLOSURE WITHOUT WRITTEN AUTHORIZATION OR THE OPPORTUNITY TO AGREE OR OBJECT

Sometimes a covered entity may use or disclose PHI without the person's written authorization and without giving the person the opportunity to agree or object. This may occur when use or disclosure is: (i) required by law; (ii) permitted by law for public health activities; (iii) related to abuse, neglect or domestic violence; (iv) for government health oversight activities; (v) for judicial and administrative proceedings; (vi) for some law enforcement purposes; (vii) about decedents to coroners, medical examiners, and funeral directors; (viii) for cadaveric organ, eye or tissue donation purposes; (ix) for research when approved by an Institutional Review Board or privacy board, when preparatory to research, or when research is on decedent's information; (x) to avert a serious threat to health or safety; (xi) for special government functions such as military activities, national security, correctional institutions about their inmates, etc.; or (xii) to comply with workers compensation laws.[25]

The provisions on use or disclosure of PHI for research purposes apply regardless of the source of funding. For example, these provisions apply both to privately and federally funded research. An Institutional Review Board (IRB) or a special privacy board may waive the written authorization requirement if the risk to individual privacy is minimal, the research could not practicably be done without the waiver and access to the PHI is essential to the research.[26]

[23] 45 C.F.R. §164.508.
[24] 164 C.F.R. § 164-512(i) explains in detail how the IRB or privacy board must handle authorization waivers for research.
[25] 45 C.F.R. § 164-512.
[26] 45 C.F.R. § 164-512(i)(1).

Some limited access for research purposes to protected health information without written authorization (or a waiver) is permitted. A researcher may access a decedent's information if the information is essential to the research. Also, a covered entity may allow a researcher preparing a research protocol access to protected health information that is necessary to the research, but the researcher may not remove any of the PHI from the covered entity. For example, the researcher could not use the PHI to contact patients to recruit them into a study. Recruitment of research subjects may become more difficult for academic research programs as a result.

Health information that is effectively de-identified is not considered protected health information. While this might be helpful with some academic research, the Rule describes eighteen identifiers that must be removed before information is considered de-identified. Removal of the identifiers would limit the usefulness of the data for most research purposes.

The covered entity may assign a code to re-identify the data if the code is not derived from information about the individual and is not shared. An alternative to this "safe harbor" is to obtain the opinion of an expert that the risk is very small that the information could be used to identify the individual.

A covered entity may disclose for research purposes a "limited data set" which excludes specific direct identifiers (names, addresses, telephones numbers, medical record numbers, or other similar identifiers). The recipient of a limited data set must sign a "data use agreement" that describes how the information will be used and that assures that it will not be further disclosed.

The Rule has transition provisions so researchers who obtained written informed consent from study participants (or an IRB approved waiver of the consent) prior to the April 14, 2003 HIPAA Privacy Rule compliance date may continue to rely on that consent without obtaining a new Privacy Rule authorization. Any changes made to such written permission after April 14, 2003, however, will require the execution of a written authorization that complies with the Privacy Rule.

PERMITTED USE OR DISCLOSURE IF THE COVERED ENTITY GIVES THE PERSON AN OPPORTUNITY TO OBJECT[27]

In some cases, health care providers may use or disclose information about patients as long as the patients have been informed of the facility's policy and have been given the opportunity to object. The notice requirement is waived for emergency circumstances, as long as the disclosure is consistent with any preference previously expressed by the individual and its disclosure is in the patient's best interest. Generally, providers may disclose to the clergy the person's name, their location in the hospital, their condition in general terms, and their religious affiliation. Except for religious affiliation, this information can also be disclosed to anyone who asks for the person by name, to friends or family who are involved in the person's care, or to identify or locate friends or family members. A covered entity may also disclose information when the individual is present and does not object.

The Rule also protects professionals who use their best judgment in allowing someone to pick up prescriptions, medical supplies, X-rays, etc. for the person. For example, a college student health center could allow a student to pick up a medical device prescribed for a family member (remember, the family member's health information may be PHI).

Covered entities may disclose information to disaster relief agencies much like they can for other emergency circumstances. Policies and procedures for handling campus disasters probably should also include a provision on handling the college's health care component disclosure of PHI to appropriate agencies.

[27] 45 C.F.R. § 164-510.

NOTICE OF PRIVACY PRACTICES[28]

The covered entity must prepare in plain language a "notice of privacy practices" that is given to individuals to inform them about how the entity handles their PHI. The notice must include a prescribed header explaining that the notice is about access to and the use and disclosure of medical information. The notice must describe (i) the types of uses and disclosures permitted for treatment, payment and health care operations purposes without written authorization; (ii) other uses or disclosures permitted without written authorization; (iii) more stringent state law restrictions on use and disclosure; and (iv) that other uses and disclosures will only be with written authorization and that the individual may revoke his/her authorization.

The notice must inform individuals of their rights and how they may exercise them and that they may request restrictions on use and disclosure but that the covered entity does not have to agree. Patients have the right to receive confidential communications about their PHI and have the right to inspect and copy their health information. They also have the right to request amendment of their PHI, to receive an accounting of disclosures, and to receive a paper copy of the privacy notice.

The notice must also (i) describe the covered entity's duties, including how individuals will be notified of changes in the policies; (ii) explain the complaint procedure; (iii) identify the entity's HIPAA contact person and how to contact them; and (iv) identify the effective date.

In the case of a College that has declared itself to be a hybrid entity, the notice will have to be prepared and used only in the health care component.

ADMINISTRATIVE RESPONSIBILITIES[29]

A covered entity has to designate someone to be responsible for developing, implementing and keeping privacy policies and procedures up to date, as well as someone who will handle complaints and respond to requests for information. For a hybrid entity, that person is appointed for the health care component(s).

Covered entity personnel (or those in the health care component of a hybrid entity) must be trained in how to handle PHI in compliance with the Privacy Rule. The current workforce has to be trained prior to the April 14, 2003 compliance date and after that, new employees must be trained within a reasonable period after joining the workforce. Changes in policies and procedures require training updates. A covered entity is required to document corrective action when members of its workforce violate its privacy policies and procedures

Although a separate Security Rule governing the security of electronic data is also pending, a covered entity under the Privacy Rule must take reasonable steps to assure the security of PHI through appropriate administrative, technical and physical safeguards. For example, a College that is covered entity would have to take reasonable administrative precautions to limit access to PHI to those who need it to carry out their job responsibilities.

The covered entity must adopt procedures for individuals to file complaints about policies and procedures or their implementation and must refrain from retaliatory action against anyone exercising their rights under the Rule or in assisting with investigations of violations.

ACCOUNTING FOR DISCLOSURES[30]

The covered entity must account for most disclosures and provide that information to the individuals who request it about themselves. Records of disclosures have to be maintained for six years, but not for disclosures where the

[28] 45 C.F.R. § 164-520.
[29] 45 C.F.R. § 164-530 .
[30] 45 C.F.R. § 164-528.

individual has signed a written authorization. Also, special arrangements have been provided for maintaining records of disclosures in large research projects where the researcher used a waiver of authorization approved by an IRB or privacy board. In those instances, a general record may be maintained revealing that the individual's PHI may have been disclosed as part of the research protocol.[31] Routine uses and disclosures for treatment, payment or health care operations purposes are exempted from the accounting requirement.

CONCLUSION

Colleges that qualify as "covered entities" may have only a few "covered functions." If so, documenting that the college is a "hybrid entity" and including these functions in the "health care component(s)" will lessen the administrative burden of implementing the Privacy Rule. If only a few areas of the campus are involved, the hybrid entity option will allow the College to treat the health care component as if it were a separate legal entity for purposes of implementing the Privacy Rule.

Even with a more limited implementation, however, a College has much work to do in order to prepare for the April 14, 2003, compliance deadline. Perhaps the most difficult implementation issues will be preparation of the required policies and procedures and training the workforce in the health care components on how to handle PHI in compliance with the Rule.

What remains, however, is dealing with the indirect impact of HIPAA on those parts of the College that may not otherwise be covered. This means that clinical education and academic research will be affected. Health professions students who obtain their clinical training at area hospitals and other health care provider sites will be affected by how those sites implement the Rule. Colleges should expect inconsistency in the early stages of implementation. One solution might be to ask state hospital associations and other trade associations or professional societies to assist in developing uniform approaches agreeable to area health care providers and the College. Even if consistency is achieved, Colleges should expect changes in how their students access and use PHI and in how their researchers acquire PHI for implementation of research protocols. Students will be held accountable for how they use and disclose PHI and may be restricted in their use of PHI outside the clinical training site. Researchers are likely to find their recruitment of clinical research participants to be more difficult.

[31] See 45 C.F.R. § 164-528(b)(4)(i).