Journal of College and University Law
2003

Article

***525** COMPLYING WITH HIPAA: A GUIDE FOR THE UNIVERSITY AND ITS COUNSEL

Pietrina Scaraglino [FNa1]

I. BACKGROUND

Colleges and universities [FN1] that provide health care or offer employee health benefits have undoubtedly spent a great deal of time and resources trying to understand and comply with their new responsibilities and obligations under privacy regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). [FN2] Although the privacy regulations were introduced as somewhat of a Congressional "after- thought," they will have a significant impact on the way covered health care providers and benefit plans at universities conduct business.

When it was passed, the primary focus of HIPAA was health insurance portability. Congress recognized that an overwhelming majority of people in the United States obtain health insurance coverage through their employers. Congress also recognized the growing frustration of Americans who felt "locked into" their jobs out of a fear that changing jobs -- whether voluntarily or as a result of economic conditions -- could mean losing their employer-based health insurance. [FN3] HIPAA addressed this problem by providing a mechanism for people to maintain their health insurance when changing jobs. [FN4] HIPAA's other aims included the prevention of healthcare fraud and abuse [FN5] and the adoption of tax-related health provisions to encourage the ***526** availability of health care. [FN6] At the time, most of the Congressional debate and commentary concentrated on these issues.

Conversely, little attention seemed focused on another provision of HIPAA entitled "Recommendations with Respect to Privacy of Certain Health Information." [FN7] Pursuant to that provision, Congress was given an opportunity to pass legislation within thirty-six months of the enactment of HIPAA "with respect to the privacy of individually identifiable health information transmitted in connection with" certain identified electronic transactions; absent Congressional action, HIPAA authorized the Secretary of Health and Human Services to promulgate regulations addressing the privacy of patient information. [FN8] The legislation or regulations were required to address at least "(1) [t]he rights that an individual who is a subject of individually identifiable health information should have[;] (2) [t]he procedures that should be established for the exercise of such rights[; and] (3) [t]he uses and disclosures of such information that should be authorized or required." [FN9]

Little guidance was given by Congress about what the future legislation or regulations should encompass. Indeed, of the hundreds of pages of Congressional reports devoted to HIPAA, [FN10] there are only a few passages that address patient privacy.

> Protecting the privacy of individuals is paramount. However, the Committee recognizes that certain uses of individually identifiable information are appropriate, and do not compromise the privacy of an individual. Examples of such

use of information include the transfer of information when making referrals from primary care to specialty care, and the transfer of information from a health plan to an organization for the sole purpose of conducting health care-related research. As health care plans and providers continue to focus on outcomes research and innovation, it is important that the exchange and aggregate use of health care research be allowed. [FN11]

In the end, Congress did not enact legislation concerning the privacy of protected health information. However, on December 28, 2000, with little initial guidance from Congress, the Department of Health and Human Services ("HHS") promulgated regulations known as "Standards for Privacy of Individually Identifiable Health Information" (the "Privacy Regulations"). [FN12] ***527** In 2001, the Bush administration re-opened the regulations for public comment and after receiving a plethora of comments, the Privacy Regulations were modified in August 2002. [FN13] Entities, including universities, who are covered by the Privacy Regulations, must be in compliance with the privacy standards by April 14, 2003. [FN14]

II. THE PRIVACY REGULATIONS: THE UNIVERSITY AS HEALTH CARE PROVIDER

While a university's primary mission is educational, there are universities who are also health care providers; universities provide health care, for instance, in clinics, in student health centers or as part of faculty practice groups of a medical or dental school. For those universities that provide health care, compliance with the Privacy Regulations has presented a real challenge.

It seems clear that in drafting and adopting the Privacy Regulations as they relate to health care providers, HHS was focused on more traditional health care providers like hospitals, dentists, doctors and other providers for whom the provision of health care is their primary responsibility. While the Privacy Regulations recognize that entities whose mission is not restricted to ***528** the delivery of health services will be covered by the Regulations, [FN15] the Regulations do not always translate well into the academic setting. In practice, the Privacy Regulations often do not take into account the manner in which health care is delivered within a college or university. The result is the imposition of a regulatory scheme that is sometimes unrealistic and difficult to adapt to an academic environment, not to mention burdensome and costly for the institutions affected.

Despite any misgivings about the application of the Privacy Regulations to the academic community, many universities are nonetheless covered by the Regulations and must take the necessary steps to comply with them. For many universities, the first step in fulfilling their compliance burdens is to establish an organizational structure to carry out the tasks necessary to achieve compliance. As an indication of the seriousness with which universities view their HIPAA obligations, some universities appoint high-level administrators, such as senior vice presidents and/or chief information officers, to oversee their HIPAA compliance efforts. Thereafter, and depending on the magnitude of the compliance effort, other individuals or committees of individuals can be appointed to direct the compliance activities in specific areas such as research or with respect to schools such as medical or dental schools. These individuals or committees can then report progress back to the responsible university administrators. It is also advisable, particularly where the compliance effort is more significant, to document what is being done by individuals or groups of individuals to achieve compliance. Once an organizational structure is in place, the necessary work can proceed to achieve compliance with the Privacy Regulations.

Depending on the size and resources of the university, a university can consider engaging an outside consultant to assist with the compliance process. There are many consultants, including law firms and others, that provide HIPAA- related services. With respect to the Privacy Regulations, these services range from assistance in analyzing whether and to what extent an entity is covered by the Regulations to assistance in drafting policies and procedures and training employees.

There are a number of key tasks that a university will face in attempting to comply with the Privacy Regulations. As will be discussed more fully below, a university must first determine whether it is a covered entity to which the Privacy Regulations apply. Next, a university must gain an understanding of the scope and depth of the Privacy Regulations and implement policies and procedures that are designed to achieve compliance with the Regulations. [FN16] In addition to policies and procedures addressing the substantive requirements ***529** of the Privacy Regulations, a university must also implement policies and procedures for handling the administrative requirements of the Regulations including the handling of complaints and the institution of sanctions against those members of its workforce who fail to comply with its policies and procedures and the Privacy Regulations. [FN17] Finally, a university must provide training to its employees on its HIPAA policies and procedures, and document that training. [FN18]

A university will likely grapple with many complicated issues as it undertakes its HIPAA compliance efforts. The purpose of this article is to identify key provisions of the Privacy Regulations, suggest approaches a university can take to achieve compliance with those provisions, and identify issues raised by the Privacy Regulations that are particularly relevant to the academic community.

A. Determining Whether the University is Covered by the Privacy Regulations

The Privacy Regulations apply to "covered entities" [FN19] ("Covered Entity"), which are health plans, health care clearinghouses and health care providers who transmit any health information in electronic form in connection with certain transactions enumerated in the Privacy Regulations ("Electronic Transactions"). [FN20] Electronic Transactions include the electronic transmission of information in connection with billing, health plan eligibility, and health plan enrollment and disenrollment. [FN21] Many universities are Covered Entities under the Regulations because they offer health care services in departments, units or schools whose staff engage in Electronic Transactions. [FN22]

Initially, a university must determine whether it provides health care while engaging in Electronic Transactions. Providing health care alone is not sufficient to trigger application of the Privacy Regulations; in order to be considered a Covered Entity, a university must provide health care services and the ***530** health care provider must perform at least one Electronic Transaction. If, for instance, a university maintains a clinic that provides health services, but the clinic does not engage in any Electronic Transactions, then the clinic would not be subject to the Privacy Regulations.

In order to determine whether a university is a health care provider subject to the Privacy Regulations, the university must examine its schools, units, and departments -- which can be numerous, decentralized and geographically scattered -- and ask key questions to determine whether health care is being provided and whether the health care providers engage in Electronic Transactions. This examination can be in the form of written questionnaires, interviews or some combination of both. For instance, a university could consider circulating a questionnaire that asks whether a health service is provided in a particular department, unit or school. The questionnaire could also list the Electronic Transactions and ask the responder to indicate which, if any, Electronic Transactions the provider engages in along with a description of the Electronic Transaction. In those cases where a health care provider who engages in Electronic Transactions is identified, the university should also determine with which, if any, other departments, units or schools in the university the health provider shares identifiable patient information. [FN23] At the end of this process, the university should have a list of all those schools, units and departments that provide health care and engage in Electronic Transactions, as well as those areas that provide support for those health care providers.

1. The University as a Hybrid Entity

Once a university determines that it engages in health care subject to the Privacy Regulations, it must determine whether it wishes to have the entire university be considered a Covered Entity or designate itself as a hybrid entity. [FN24] A "hybrid entity" under the Privacy Regulations is defined as a legal entity that is a Covered Entity (i.e., it is a HIPAA-covered health plan, health care provider or clearinghouse) "[w]hose business activities include both covered and non-covered functions." [FN25] Because universities that provide health ***531** care services also -- indeed primarily -- engage in activities that are not covered by the Privacy Regulations, they always have the option of declaring themselves a hybrid entity under the Privacy Regulations.

Certain benefits flow to the university when it declares itself a hybrid entity. First, the obligations imposed under the Privacy Regulations apply only to the covered components of the hybrid, [FN26] and the university may have an interest in confining the application of those regulations only to the covered components. For instance, a university may have a clinic within the university that provides health care but does not engage in Electronic Transactions. If the university elects to designate itself a hybrid entity, then the clinic would not be identified as a covered component; conversely, if the university does not elect to designate itself as a hybrid entity, then the clinic would be part of the Covered Entity and, thus, subject to the Privacy Regulations. Second, while it may be worthwhile for a university to provide all of its employees with a certain amount of HIPAA training, it must provide training to all employees of the covered components. [FN27] By electing not to designate itself as a hybrid entity, a university may be expanding its training obligations under the Privacy Regulations. Finally, to the extent that the Privacy Regulations apply to part or all of a university, sanctions -- both criminal and civil -- for violation of those Regulations will also apply. [FN28]

The benefits of declaring a university a hybrid entity must be weighed against the consequences of that declaration which could present logistical and other problems for a university. For instance, "[a] hybrid entity is required to create adequate separation, in the form of firewalls, between the health care component(s) and other components of the entity." [FN29] For those universities in which the delivery of health care is a substantial activity, it may be logistically difficult to separate out and create firewalls between those parts of the university that engage in HIPAA-covered activities and those that do not. In addition, covered components of a hybrid entity may not share information with the non-covered components of the entity unless specifically permitted by the Privacy Regulations. [FN30] As a result, a university may determine that impeding the flow of patient information from a covered component ***532** of its potential hybrid to another non-covered component would be unworkable or burdensome.

Where a university decides to declare itself a hybrid entity, it must identify the components of the university that provide health care and engage in one or more Electronic Transactions. For instance, the faculty practice offices and clinics of a school of medicine or dental college will likely be covered components of a university. [FN31]

In addition, a university should identify those areas of the university that provide support services to the covered components that involve the sharing of patient-specific health information. In order for health information to continue to flow to support areas, the departments providing support must be declared covered components of the hybrid to the extent that their services would make them a business associate of the covered component if they were separate entities. [FN32] If those areas were not included as part of the hybrid entity, then the covered components would likely need individual authorizations [FN33] before patient health information could be shared. [FN34] An example of a covered support office might be a university's in- house counsel's office that may perform services for covered components that involve the sharing of health information; in-house counsel may review medical records prior to release pursuant to a subpoena or be available to consult with employees in the covered component about legal issues that might involve the exchange of health information. Similarly, a university's office of information technology ***533** may perform services on behalf of a covered component

that might involve the disclosure of patient health information to the information technology staff. If those units -- legal counsel and information technology -- are designated as covered components of the hybrid entity, then patient health information may flow freely between the health care providers and those units subject, of course, to the requirements of the Privacy Regulations. Conversely, if those units are not identified as covered components, then the covered components may release patient health information to support areas that are not covered components only with a patient's written authorization. [FN35]

Once a university identifies those components that provide HIPAA- covered health care and that provide support services for the health care components that would otherwise create a business associate relationship if the components were separate legal entities, the university must declare itself a hybrid entity and maintain that declaration in written or electronic form. [FN36] In order to accomplish this, a university's board of directors could pass a resolution declaring the university a hybrid and identifying the covered components. In order to allow the university some flexibility in amending its hybrid declaration to recognize "new" covered components that might develop in the future, [FN37] the resolution or other written declaration should identify a high-level administrator with authority to amend the declaration or set forth another process for amending the declaration.

2. The University as Part of an Organized Health Care Arrangement

Once a university determines that it is a Covered Entity under HIPAA, it should also examine whether it might be delivering health care as part of an "organized health care arrangement" ("OHCA"). [FN38] Under the Privacy Regulations, an OHCA means a "clinically integrated care setting in which individuals typically receive health care from more than one health care provider." [FN39] In addition, an OHCA under the Privacy Regulations can be "[a]n organized system of health care in which more than one covered entity participates, and in which the participating covered entities ... [h]old themselves out to the public as participating in a joint arrangement" [FN40] and participate ***534** jointly in at least one of the following: utilization review, [FN41] quality assessment and improvement activities [FN42] or certain payment activities. [FN43]

Universities may determine that they participate in an OHCA under a number of different circumstances. For instance, for universities with medical or dental schools, faculty at those schools might deliver health care in a hospital that is affiliated with the university; patients coming to the hospital believe that they are being treated by the "hospital" and may have no understanding that the physicians treating them are actually employees of the school. In addition, a medical school may have a relationship with an affiliated hospital in which the two entities hold themselves out to the public as an integrated unit and engage in joint quality assessment and improvement activities. In either case, a university and its health care "partner" constitute, and could elect to act as, an OHCA.

One of the primary benefits to a university in recognizing its participation in an OHCA is that the university and other member(s) of the OHCA are permitted to use a joint notice of privacy practices and to share Protected Health Information ("PHI") for joint operations of the OHCA as if they were a single Covered Entity. [FN44] The alternative would be almost unworkable: to have the separate Covered Entities independently undertake their privacy obligations in a health care setting in which the patient does not necessarily view the health providers as separate and distinct. [FN45]

Unlike the hybrid declaration, the Privacy Regulations contain no requirement that a university document its participation in an OHCA by written agreement or other written documentation. Because the Covered Entities ***535** participating in an OHCA must, at the very least, agree to abide by the terms of the joint notice, [FN46] a university should reach out to the other OHCA participants so that the Covered Entities can come to a meeting of the minds as to the identity of the OHCA, the consequences of the OHCA "designation," and the content of the joint privacy notice. Although not required by the Privacy Regulations, it is more prudent for a

university to document in some manner the common understanding of the OHCA participants so no misunderstandings occur later. For instance, the parties to an OHCA could enter into a memorandum of understanding or letter agreement to memorialize their common understanding.

B. The Use and Disclosure of PHI

1. What is PHI?

The basic and broad tenet of the Privacy Regulations is that Covered Entities may not use or disclose protected health information except as specifically permitted or required by the Privacy Regulations. [FN47] PHI is individually identifiable health information [FN48] defined as any information maintained or transmitted in any media relating to an individual's past, present or future physical or mental condition (including the payment or provision of health care with respect to the individual), that identifies or may reasonably lead to the identification of the individual and that is created or received by a Covered Entity or employer. [FN49] In order to comply with the Privacy Regulations, universities must understand what information held by them is considered PHI.

a. Specific Exclusions from the Definition of PHI

Universities may hold three important categories of health information that are specifically excluded from the definition of PHI. First, a university's ***536** employment records that it holds as an employer are not considered PHI and thus not subject to the Privacy Regulations. [FN50] For example,

> [M]edical information needed for an employer to carry out its obligations under FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees, may be part of the employment records maintained by the covered entity in its role as an employer. [FN51]

Accordingly, to the extent that a university (or component of a university) holds employee health information in its employment files, that information is not subject to the Privacy Regulations. [FN52]

A university must always be aware of the context in which it holds particular PHI since the PHI it holds as a Covered Entity -- which can be the same information it holds as an employer -- continues to be protected by the Privacy Regulations.

> For example, drug screening test results will be protected health information when the provider administers the test to the employee, but will not be protected health information when, pursuant to the employee's authorization, the test results are provided to the provider acting as employer and placed in the employee's employment record. Similarly, the results of a fitness for duty exam will be protected health information when the provider administers the test to one of its employees, but will not be protected health information when the results of the fitness for duty exam are turned over to the provider as employer pursuant to the employee's authorization. [FN53]

***537** In some universities, the student health center may administer drug screening or fitness for duty exams for the university's employees. Assuming that the student health center is covered by the Privacy Regulations, when the employee goes to the health center, the employee's PHI is protected under the Privacy Regulations. As a result, the health center cannot release the PHI to the university (of which it is a part) acting as employer without an authorization from the employee. Once the PHI is released by the health center in compliance with the Privacy Regulations, the information held by the university as employer is not considered PHI and is thus not covered by the Privacy Regulations.

The second and third categories of health information that are specifically excluded from the definition of PHI are of particular importance to universities. Education records covered by the Family Educational Rights and Privacy Act ("FERPA") [FN54] and those student medical records excluded by FERPA [FN55] are not considered to be PHI subject to the Privacy Regulations. [FN56] No records are covered by both the Privacy Regulations and FERPA. And, interestingly, the student medical records excluded by FERPA are covered by neither FERPA nor HIPAA. Accordingly, universities may continue to treat their student records as they traditionally have in accordance with FERPA and state law. [FN57]

b. De-Identified Information

Where health information does not "identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual," such information is not PHI ("De-identified Information"). [FN58] Accordingly, De-identified Information can be used and disclosed freely and is not subject to the Privacy Regulations. [FN59] A university may, where possible, find it useful and appropriate to consider the use or disclosure of De-identified Information.

A university can employ two methods to determine whether health information is not individually identifiable and, thus, De-identified Information. First, a "person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" [FN60] can review the health information and ***538** determine "that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information." [FN61] Second, a university can itself de-identify (or can retain a business associate to de-identify) health information by removing eighteen specific identifiers from the information including name, geographic information except for the first three digits of a zip code, telephone numbers, social security numbers, email addresses, dates (except year) related to an individual, and medical record numbers. [FN62] Even with this laundry list of identifiers removed, PHI still is not De-Identified Information unless the Covered Entity "does not have actual knowledge that the information could be used alone or in combination with other information to identify [the individual]." [FN63]

A university may find it useful in the context of student training to use De-Identified Information. For instance, a university's faculty practice office might permit students (from its university or other universities) to train in its offices. As part of their training, students may need to take information from the faculty practice office back to the classroom for discussion and analysis. While the student may not remove identifiable patient information from the practice setting, a university could permit the student to remove De-Identified Information. [FN64]

2. Permitted Uses and Disclosures of PHI

The Privacy Regulations set forth standards regarding the permitted uses and disclosures of PHI including under what circumstances PHI must be used or disclosed and under what circumstances PHI may be disclosed. Universities must understand the requirements of the Privacy Regulations and develop and implement policies and procedures designed to achieve compliance with those requirements. [FN65]

***539** The policies and procedures developed and implemented will depend upon the size of the university's health care components and the kinds of activities engaged in with respect to PHI. [FN66] These factors will also influence how a university attempts to develop and implement policies. For instance, where a university's health care components are relatively limited in size and scope, policies and procedures may be developed internally. Conversely, where a university's health care components are relatively large or where there exists more than one health care component, it may be helpful for a university who can afford it to engage a

consultant who can draft policies and procedures specific to the covered components of the university. Although engaging a consultant may ease the burden on the staff who work in the covered components of a university, it does not obviate the need for involvement of those employees since it is those employees who are best able to evaluate the efficacy of the policies and procedures in the context of day-to-day operations.

a. Mandatory Disclosure: Individual Requests and HHS

The Privacy Regulations require universities to disclose PHI in a number of instances. A university must disclose PHI to an individual when the individual requests access to her or his PHI [FN67] or when an individual requests an accounting of disclosures of her or his PHI. [FN68] A university must also disclose PHI to HHS in order to allow HHS to investigate or determine the university's compliance with the Privacy Regulations. [FN69] A university's policies and procedures should reflect these situations that require mandatory disclosure.

b. Permitted Use and Disclosure: Treatment, Payment, Health Care Operations and Incidental Disclosures

In general, a university may use or disclose PHI for treatment, [FN70] payment ***540**[FN71] or health care operations ("TPO"). [FN72] As a practical matter, then, universities may use PHI for most, if not all, of their treatment and business needs. For instance, a health care provider can share PHI with other providers within the university who are involved in a patient's care or with another provider outside the university to whom the patient may have been referred. A university can also share PHI with an individual's insurance company in order to assist the university in obtaining reimbursement for an individual's treatment or to obtain pre-certification for an individual's treatment. Finally, a university can use PHI in order to conduct business operations such as the evaluation of the performance of staff or the education of staff in order to help improve the quality of care they provide.

In addition, so long as a university has applied reasonable safeguards to protect PHI and implemented the minimum necessary standard as required by the Privacy Regulations, [FN73] a university may use or disclose PHI incident to a use or disclosure otherwise permitted by the Privacy Regulations. [FN74]

For example, a provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room. Assuming that the provider made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental disclosure resulting from such conversation is permissible under the Rule. [FN75]

***541** Contrary to fears raised when the Privacy Regulations were first published, universities need not retrofit their facilities to ensure that there is no possibility that PHI will be disclosed. [FN76] Moreover, so long as reasonable safeguards are in place to limit the amount of PHI disclosed, health care providers can continue to use sign-in sheets and call out patients' names in the waiting room. [FN77] Similarly, health care providers can continue to leave messages on answering machines or with family members to remind a patient of an appointment so long as the information left is limited. [FN78]

Notwithstanding the foregoing, universities should examine their facilities and take reasonable steps to safeguard PHI from incidental disclosure. For instance, computer screens which contain PHI should be positioned so that they are not easily seen by the public. In addition, it may be prudent for universities to implement policies and procedures with respect to the transmission of PHI by fax or email to ensure that reasonable safeguards are in place to protect the PHI. For instance, a university could decide that it will limit the transmission of PHI by fax or email or prohibit such transmission altogether. Alternatively, a university could adopt procedures requiring verification of the recipient of an email or fax and/or the

transmission itself.

Once again, a university must develop and implement policies and procedures that reflect these standards. [FN79] Specifically with respect to the development of procedures, it is recommended that a university examine the flow of PHI within its covered components to ensure that its procedures provide a reasonable balance between the requirements of the Privacy Regulations and the necessary use of PHI in day-to-day operations.

c. Permitted Use and Disclosure of PHI: Pursuant to Individual Authorization

Universities may disclose PHI pursuant to an authorization that meets the requirements of the Privacy Regulations and the disclosure must be only as ***542** permitted pursuant to the authorization. [FN80] In general, universities may not condition treatment and payment on the provision of an authorization. [FN81] An individual may revoke an authorization previously given except to the extent that a university has already taken any action in reliance on the authorization. [FN82]

In order for an authorization to be valid under the Privacy Regulations, it must be written in plain language [FN83] and contain at least the following six elements:
(1) A description of the information to be used and disclosed. The description must identify the information "in a specific and meaningful fashion"; [FN84]
(2) The name of the person authorized to make the disclosure; [FN85]
(3) The name of the person(s) to whom the disclosure can be made; [FN86]
(4) A description of the purpose of the requested disclosure. Where an individual initiates the authorization, it is sufficient that the disclosure state that information is to be disclosed "at the request of the individual"; [FN87]
(5) An expiration date or event. Where the authorization is for the use and disclosure of PHI for research, the authorization can indicate that there is no expiration date or that the authorization will expire at the end of the research study; [FN88] and
(6) Signature and date. [FN89]

In addition, the authorization must contain statements adequate to place an individual on notice that (1) the individual has the right to revoke the authorization in writing, and any exceptions to the right as permitted by the Privacy Regulations, [FN90] (2) treatment and payment may or may not, as the ***543** case may be, be conditioned on the provision of an authorization, [FN91] and (3) information disclosed pursuant to an authorization may potentially be re-disclosed by the recipient of the information and no longer protected by the Privacy Regulations. [FN92]

A university should take steps to insure that, where required, PHI is disclosed pursuant to a valid authorization. First, a university should draft, and have available, its own compliant form of authorization. [FN93] Where a health care provider already uses some form of authorization to release medical information, the form currently in use can be reviewed and modified to ensure that it contains the elements set forth above which are required by the Privacy Regulations.

Second, a university should examine the manner in which requests for the release of health information are currently handled. The procedures currently in place can likely continue to be used with modifications to ensure compliance with the Privacy Regulations. For instance, in order to ensure that PHI is disclosed only in accordance with a valid HIPAA authorization, a university can prepare a simple checklist that lists those elements necessary in a HIPAA- compliant authorization as well as the required statements. [FN94] Thereafter, the university's procedures can require that designated personnel review authorizations that are received against the checklist to ensure that they contain the required elements and to ensure that the expiration date noted on the authorization has not passed; [FN95] if an authorization is not valid, ***544** the procedure can require that the invalid authorization be returned along with the university's valid form that the individual can be directed to complete and return. A university's procedures should also set forth a mechanism for maintaining authorizations received for six years, [FN96]

including the place where the authorizations will be stored. For instance, a university could decide to maintain authorizations as part of an individual's medical record or in a separate "authorization" file.

d. Permitted Use and Disclosure: Where an Individual is Given an Opportunity to Agree or Object

Two broad categories of use and disclosure of PHI are permitted so long as an individual is informed in advance and has the opportunity to agree to, prohibit, or restrict the use or disclosure: uses and disclosures for facility directories and uses and disclosures for involvement in the individual's care and notification purposes. [FN97] Universities may inform individuals orally of the intended use or disclosure and the individual's agreement or objection to the use or disclosure may be obtained orally as well. [FN98]

i. Facility Directory Information

Unless an individual objects, a university may use PHI such as the individual's name, location, and general condition to maintain a directory of individuals at its facility. [FN99] The directory information may then be disclosed to members of the clergy or people who ask for the individual by name. Prior to use and disclosure of such information, however, a university must inform an individual of the intended use and provide the individual with an opportunity to restrict or prohibit some or all of the uses and disclosures. [FN100]

Only those universities that maintain hospitals or other such facilities need to draft and implement policies and procedures that address the use and disclosure of PHI for purposes of maintaining a facility directory. Where such policies and procedures are necessary, a university should put a mechanism in place for informing individuals of the PHI it intends to use and to whom it will be disclosed. In addition, a university will need to establish procedures for obtaining and recording an individual's desire to restrict or prohibit the disclosure of some or all of the information, and for communicating the individual's wishes to the appropriate staff whose job it is to release such information. Needless to say, universities may face logistical difficulties creating a system that can successfully record an individual's particular desires and convey ***545** those desires to staff on an individual basis. For instance, while it may be easy enough to delete an individual's name completely from a facility directory, it may present more serious operational issues to ensure that an individual's desire to have only one piece of information (for instance, location) suppressed.

ii. Involvement in Individual's Care

The Privacy Regulations attempt to address the common situation in which individuals want health care providers to provide medical information to family and friends who may accompany them to appointments or telephone for information on their behalf. Pursuant to the Privacy Regulations, in those cases where an individual agrees or does not expressly object, or where the university's health care providers can reasonably infer based on their professional judgment that the individual does not object, a university may disclose PHI to a family member, relative, close personal friend or any other person identified by the individual. [FN101] Indeed, the Privacy Regulations specifically permit providers within a university to use their professional judgment "and ... experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of" PHI. [FN102] For instance, if a child with an elderly parent calls her parent's doctor to discuss her parent's medical condition in order to ensure that the parent's health needs are being met, a physician can speak with the child without violating the Privacy Regulations. [FN103] Again, a university should devise and implement policies and procedures that reflect these

permitted uses and disclosures of PHI. [FN104]

***546** e. Permitted Use and Disclosure: Individual's Agreement or Objection Not Required

The Privacy Regulations address a host of other situations in which a university may use or disclose PHI without an individual's authorization or the opportunity for the individual to agree or object to the disclosure. [FN105] These include uses or disclosures of PHI as required by law, [FN106] for public health activities, [FN107] in connection with abuse, neglect, or domestic violence, [FN108] for health oversight activities, [FN109] for judicial and administrative proceedings, [FN110] for law enforcement purposes, [FN111] about decedents, [FN112] for cadaveric organ, eye, or tissue donation purposes, [FN113] for research purposes, [FN114] to avert a serious threat to health or safety, [FN115] for specialized government functions, [FN116] and for workers' compensation. [FN117] Each category of permitted use and disclosure of PHI carries with it its own special (and sometimes complicated) provisions and requirements for when such PHI may be released, under what circumstances, and to whom.

A university should familiarize itself with the different circumstances under which PHI may be used or disclosed without an individual's authorization or the opportunity for the individual to agree or object to the disclosure and create policies and procedures that address the unique requirements associated with such uses and disclosures. For instance, it may not be uncommon for a university to be required to use and disclose PHI for research purposes, for health oversight purposes, for public health activities, as required by law, or for judicial and administrative purposes. It is particularly important that a university's policies and procedures be well developed with respect to these uses and disclosures of PHI since a university will more routinely encounter them in its daily operations.

3. What PHI Can Be Disclosed: Minimum Necessary Standard

When a university uses or discloses PHI or requests PHI from another Covered Entity, it "must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." [FN118] However,

***547** This is not an absolute standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information. [FN119]

Importantly, there are circumstances under which the "minimum necessary standard" does not apply. Such circumstances include disclosures to or requests by a health care provider for treatment, uses or disclosures to the individual, and disclosures made pursuant to an authorization. [FN120] Although disclosures between health care providers for treatment purposes are not subject to the minimum necessary standard, other uses of PHI for payment and health care operations -- such as use of PHI for billing -- are not exempt from the standard. [FN121]

A university must develop and implement policies and procedures to ensure compliance with the minimum necessary standard. As part of this process, a university must examine its workforce and identify those employees within the university who require access to PHI in order to do their jobs, as well as the kinds of PHI to which those employees require access. [FN122] The university must then put procedures in place that ensure that particular employees obtain access to only that PHI necessary for the employee to do her or his job. [FN123]

***548** A university must also develop and implement policies and procedures for both routine and non-routine disclosures and requests of PHI. For those routine and recurring disclosures and requests, like disclosures required for billing, the

university can develop a written protocol identifying the minimum disclosure or request of PHI necessary to accomplish the identified routine and recurring task. [FN124] A university must also put into place a procedure for handling other, non-routine requests and disclosures. [FN125] For instance, a university may choose to identify a particular employee by title within an office or department, or a specific office within a larger department or unit, who can review the disclosure or request. The review would be conducted in accordance with specific criteria the university develops for insuring that the minimum necessary PHI is disclosed or requested. [FN126]

4. To Whom May PHI be Disclosed: Business Associates and Personal Representatives

The Privacy Regulations specifically address disclosure of PHI to two important classes of people and entities: individuals and personal representatives and a university's business associates. The Privacy Regulations also permit use of PHI by, and disclosure to, a university's business associates.

a. Business Associates

A business associate is a person or entity who, on behalf of a Covered Entity or OHCA (other than as a member of the workforce), [FN127] performs or assists in the performance of a "function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, [sic] processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing." [FN128] In addition, a business associate of a Covered Entity is a person or entity who provides "legal, actuarial, accounting, consulting, data aggregation ..., management, administrative, accreditation, or financial services ... where the provision of the service involves the disclosure of individually identifiable health information ...." [FN129]

In order to share PHI with a business associate, a university must obtain the business associate's "satisfactory assurance that the business associate ***549** will appropriately safeguard the information." [FN130] This does not apply "[w]ith respect to disclosures by a [university] to a health care provider concerning the treatment of [an] individual." [FN131] The assurances of a business associate can be obtained in a "contract or other written agreement or arrangement," so long as the form meets the requirements of the Privacy Regulations. [FN132] Generally, a university will likely obtain assurances from a business associate either through a written amendment to an existing written agreement or through a separate business associate agreement.

The Privacy Regulations set forth a host of issues that the business associate agreement [FN133] must address, including (a) the permitted uses and disclosures of PHI by the business associate, (b) obligations of the business associate including its agreement not to use PHI other than as permitted in the business associate agreement, to safeguard the PHI, to make PHI available for amendment if necessary, and to make its books and records available to HHS for purposes of determining the Covered Entity's compliance with the Privacy Regulations, and (c) the Covered Entity's right to terminate the business associate agreement if the Covered Entity determines that the business associate has violated a material term of the agreement. [FN134] Although a university that enters into a business associate agreement with a business associate is not required to monitor the business associate's compliance with the agreement, if a university knows of "a pattern of activity or practice of the business associate that constitute[s] a material breach or violation of the business associate's obligation under the contract or other arrangement," the university must take reasonable steps to cure the breach or end the violation and, if unsuccessful, terminate the agreement, if feasible, or if termination is not feasible, report the problem to HHS. [FN135]

Universities that provide extensive health care services face a formidable task in

identifying their business associates and ensuring that they have a business associate agreement in place with each business associate. Initially, a university should identify all of its potential business associates. Some common examples of business associates of universities include medical transcription services, outside legal counsel, outside accounting firms, consultants who have access to PHI, outside billing companies, software licensing companies or companies that provide systems and have access to PHI, medical records storage and archiving companies, and copy services. Contrary to what some ***550** thought when the Privacy Regulations were initially published, persons or entities who perform janitorial, plumbing, electrical and other such services for a university's covered components are not considered business associates. A business associate contract is not required "[w]ith persons or organizations (e.g., janitorial services or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all." [FN136] Given its importance to the academic community, it should also be noted that a researcher is not a business associate of a Covered Entity for purposes of performing research, either with patient authorization, pursuant to a waiver or as a limited data set. [FN137] In that situation, the researcher is not conducting any activity, such as payment or health care operations, subject to the Privacy Regulations. [FN138]

When attempting to identify business associates, there may be instances in which a university can elect to treat a business associate as part of its own workforce where the work performed by the business associate is under the direct control of the university. In that case, no business associate agreement is necessary between the would-be business associate and the university. For instance, a university may hire someone on a part-time, contract basis to oversee a particular health care function or it may hire workers from an agency to provide coverage or other temporary services. In those cases, the university can elect to treat those workers as part of its workforce, rather than as business associates. By choosing to treat such individuals as part of its workforce, however, the university may become responsible for the actions of, and potential HIPAA violations by, those workers.

Depending on the size of a university's health care operations, the task of identifying the business associates of a university's covered components may be daunting. One way to accomplish this is by providing some background training (for instance, by providing an outline) to those departments or offices, which are part of the covered component of the university, explaining what a business associate is and giving them some examples. Those departments or offices can then be provided with a chart that asks them to identify possible business associates including the business associates' names, addresses, and contact information as well as a brief description of the service provided (so that a determination can be made about whether the identified entity is truly a business associate), whether there is an underlying agreement with the business associate and, if so, the termination or renewal date. At that point, the university will be able to evaluate who its business associates are and when it must have a business associate agreement in place. In addition, the staff of the relevant covered components of the university must be trained to identify business associates as new relationships are entered into with third parties.

***551** Once a university identifies its business associates, it must undertake to secure business associate agreements with them. [FN139] To help accomplish this, a university should develop a standard form business associate agreement that can be used throughout the university. A university can choose to draft its own form agreement based on the requirements of the Privacy Regulations. In addition, HHS has made available a sample form business associate agreement, which a university can use in its entirety or modify to suit its own needs. [FN140] Finally, standard HIPAA forms, including forms for business associate agreements, can be purchased from consultants, including many law firms. [FN141]

b. Personal Representatives

The Privacy Regulations recognize that there may be times when individuals may not

be able to receive information about their health care or otherwise exercise their rights due to, for instance, legal or medical incapacity. Accordingly, the Privacy Regulations mandate that persons other than the individual, defined as "personal representatives," be treated as the individual for purposes of the Privacy Regulations. [FN142] "The personal representative stands in the shoes of the individual and has the ability to act for the individual and exercise the individual's rights." [FN143] While the Privacy Regulations recognize the right of a personal representative to act on behalf of an individual for purposes of the Regulations, the scope of the personal representative's ***552** right and authority to act on the individual's behalf is determined under applicable state law. [FN144]

A university's policies and procedures must reflect its requirements with respect to personal representatives, including verification of the person's status as personal representative under applicable law. In addition, the university's policies and procedures must reflect the special requirements imposed by the Privacy Regulations on personal representatives for adults and emancipated minors, [FN145] unemancipated minors, [FN146] deceased individuals, [FN147] and individuals who have suffered abuse, neglect, or endangerment. [FN148]

C. Other Obligations of a University Under the Privacy Regulations

Universities have other obligations under the Privacy Regulations with respect to PHI and the delivery of health care. For instance, universities must designate privacy officials and provide individuals with a notice of privacy practices, provide individuals with access to their PHI, and provide individuals with accountings of disclosures of their PHI. Universities must develop policies and implement procedures to fulfill these obligations under the Privacy Regulations.

1. Designation of Privacy Officer

Universities are required to designate a privacy official "who is responsible for the development and implementation of the policies and procedures" of the university with respect to compliance with the Privacy Regulations. [FN149] In addition to assisting in the development of policies and procedures, a privacy officer's job description may include participation in the development, implementation, and on-going HIPAA training, acting as privacy consultant to all affected areas of the university, working with affected areas to oversee the enforcement of patient rights, and ensuring that the covered components of the university maintain and enforce their privacy policies and procedures. [FN150]

In addition to a privacy official, a university must also designate a person or office "who is responsible for receiving complaints" about a university's alleged noncompliance with the Privacy Regulations. [FN151] Depending upon the particular needs of a university, the privacy official and the person designated ***553** to receive HIPAA complaints on behalf of the university can be the same person. In addition, the Privacy Regulations do not require that the privacy official's position be full-time. Accordingly, a university must assess the parameters of the privacy officer's responsibilities in light of the size and complexity of the covered components of the university and the university's resources to determine the nature of the privacy position it creates.

For instance, universities that have diverse covered components (i.e., a medical school, dental school, or student health center) might consider appointing a full-time university-wide privacy officer, who could also handle complaints. Alternatively, a university could designate a university-wide privacy officer -- either part-time or as part of the responsibilities of an existing employee -- along with designated privacy officials at each of the covered components. This might make particular sense where the covered components are each large parts of the university that do not generally interact very much with each other in day-to-day activities. Indeed, it might be beneficial for the university to have a privacy official at each of the covered components who is intimately familiar with the staff at the covered

component and how health care is delivered at the covered component. Whatever a university decides, the privacy officer designation must be reasonable based on the responsibilities of the university under the Privacy Regulations.

2. Notice of Privacy Practices

In general, universities are required under the Privacy Regulations to provide individuals with "adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information" ("Notice of Privacy Practices"). [FN152] The Notice of Privacy Practices must be written in plain language [FN153] and (a) describe, and give examples of, the uses and disclosures of PHI in which the Covered Entity will engage, [FN154] (b) "[i]f the [C]overed [E]ntity intends to engage in" fundraising ***554** or "contact the individual to provide appointment reminders or information about treatment alternatives or other health ... benefits and services," include a statement to that effect, [FN155] (c) "contain a statement about the individual's rights with respect to [PHI]" including the individual's right to amend PHI, access PHI, and receive an accounting of the Covered Entity's uses and disclosures of PHI, [FN156] (d) contain a statement about the Covered Entity's duties with respect to PHI, including the legal requirement to maintain the privacy of PHI and abide by the terms of the Notice of Privacy Practices, [FN157] (e) contain a statement concerning individuals' rights to complain with respect to alleged violations of their privacy rights, [FN158] and (f) set forth "the name, or title, and telephone number of a person" from whom to obtain further information. [FN159]

A university that provides health care, then, must design its own Notice of Privacy Practices that describes its particular uses and disclosures of PHI and contains the other information required by the Privacy Regulations. For universities that provide health care in different settings -- for instance, in one or more faculty practice settings, dental clinics and/or student health centers -- it may even be necessary to draft different Notices tailored to the particular health care setting. Given all that must be included in a university's Notice of Privacy Practices, it is common for the Notice to total ten or more pages. Providers have, with good reason, raised concerns about providing individuals with such a lengthy document; understandably, providers do not want to cause undue anxiety among the individuals who come to them for care and treatment. Accordingly, a university might consider providing individuals with a "layered notice" of their privacy rights. "For example, a [university] may satisfy the notice requirements by providing the individual with both a short notice that briefly summarizes the individual's rights, as well as other information; and a longer notice, layered beneath the short notice, that contains all of the elements required by the Privacy Rule." [FN160]

Once a university drafts its Notice of Privacy Practices, the Notice must be provided to individuals on the "date of the first service delivery" [FN161] or, in ***555** cases of emergency, "as soon as reasonably practicable after the emergency treatment situation," [FN162] and the university's policies and procedures should reflect that reality. In addition, a university's policies and procedures should require that the staff responsible for providing the Notice make a good faith effort to obtain the individual's acknowledgement that she or he has received the Notice. The acknowledgement can be a statement on a separate sheet of paper that the individual can be asked to sign; in those cases where a university is also required under state law to obtain consent from the individual for the use and disclosure of PHI, the university can elect to combine the consent and acknowledgement forms so long as that practice is not prohibited by relevant state law. If the acknowledgement is not obtained, the staff person should be required to "document its good faith efforts to obtain such acknowledgement and the reason why the acknowledgement was not obtained[.]" [FN163] One method for documenting the refusal is to instruct staff to note on the acknowledgement form their efforts to obtain the individual's signature and the reason(s) why they were unsuccessful. A university's policies and procedures should also require that acknowledgements and documented efforts to obtain acknowledgements be retained by the university for six years; [FN164] a university could decide to retain such documents in the individual's

medical record or in a separate file. Finally, in addition to providing individuals with a Notice of Privacy Practices, a university must also prominently post the Notice in its facilities and make the Notice available to individuals who request it. [FN165]

When there is a material change in the way in which a university uses and discloses PHI, a university must revise its Notice of Privacy Practices and distribute the new Notice. [FN166] The new Notice must be posted in the provider's ***556** office and provided to individuals upon request. [FN167] Importantly, the university is not required to provide the new Notice to individuals who have already received the provider's Notice of Privacy Practices. [FN168]

3. Individual's Access to PHI

In general, individuals have a right to inspect and "obtain a copy" of their PHI [FN169] in the designated record set. [FN170] A university may require that requests for access to PHI be made in writing so long as individuals are informed of that requirement. [FN171] A university must, in general, act on an individual's request for access to PHI within thirty days of a request. [FN172] Action may include informing the individual that the university requires an additional thirty days in which to respond to the request. [FN173] Universities must draft and implement policies that permit access to PHI by individuals as required by the Privacy Regulations. In addition, universities must develop processes for carrying out those policies. For instance, a university should designate a person or persons who will be "responsible for receiving and processing requests for access" to PHI. [FN174]

Under certain circumstances -- for instance, when access is requested during the course of a research project -- a university may deny an individual access to PHI. [FN175] While certain denials of access are not reviewable by the individual, there are specified situations -- for instance, when a licensed health care professional determines that the requested access is reasonably likely to endanger someone's life or physical safety -- under which an individual may ask for a review of a university's decision to deny access to the ***557** individual's PHI. [FN176] A university must also establish a mechanism for reviewing denials of access to PHI as required by the Privacy Regulations, and possible state law, including designating a licensed health care professional not involved in the original denial of access, to whom requests for review can be referred. [FN177]

4. Accounting of Disclosures

An individual has a right to an accounting of the disclosure of her or his PHI made for a period of time up to the last six years prior to the request (but not prior to April 14, 2003). [FN178] However, a university does not have to account for certain uses and disclosures, including disclosures to carry out treatment, payment, and health care operations, disclosures to individuals about themselves, disclosures pursuant to an authorization, [FN179] and incidental disclosures. [FN180] Examples of the types of disclosures that must be accounted for include disclosures for research (other than with a patient's authorization or as part of a limited data set), [FN181] disclosures about victims of abuse, neglect, or domestic violence, disclosures for judicial or administrative proceedings, disclosures for law enforcement purposes, [FN182] and disclosures in connection with workers' compensation.

A university must establish policies and procedures that ensure that uses and disclosures subject to the accounting rules are tracked. A university may decide to track all relevant uses and disclosures in a patient's medical record. Alternatively, a university can track relevant uses and disclosures in a centralized database. In either case, the university's procedures must clearly indicate ***558** what repository of information must be checked prior to responding to a request for an accounting.

Once a university receives a request for an accounting and gathers the relevant information, the university must provide the individual with a written accounting of disclosures. [FN183] The written accounting must include the date of disclosure, the name of the entity or person who received the PHI and, if known, the address, a brief description of the PHI disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, the written request for disclosure. [FN184] In response to concerns raised by the research community that providing such information would be overly burdensome, the August 2002 Modifications changed the requirements for the content of accountings where a disclosure is made for a research purpose for fifty or more individuals. [FN185] In that case, the university need only include in its accounting

> (A) [t]he name of the protocol or ... research activity[,] (B) [a plainly written description] of the research protocol or ... activity, including the purpose of the research and the criteria for selecting particular records[,] (C) [a] brief description of [the PHI] disclosed [,] (D) [t]he date or [time period of the disclosure], including the date of the last ... disclosure[,] (E) [t]he [identity] of the entity that sponsored the research [as well as] the researcher to whom the information was disclosed[,] and (F) [a] statement [about whether the individual's PHI] may or may not have been disclosed for a particular ... research purpose. [FN186]

A university's procedures must reflect the fact that it must act on an individual's request for an accounting within sixty days; it can obtain an extension of another thirty days if it notifies the individual of the delay within the sixty-day period. [FN187] A university must provide the first accounting requested by an individual in a twelve-month period without charge; thereafter, the university "may impose a reasonable, cost-based fee for each subsequent request ***559** for an accounting" if the university tells the individual in advance about the charge and provides her with an opportunity to withdraw her request. [FN188]

5. Requests for Amendment of PHI and Additional Protections

The Privacy Regulations also permit individuals to ask universities to amend their PHI and/or afford them additional privacy protections. [FN189] The Privacy Regulations set forth under what circumstances individuals may request that their PHI be amended [FN190] or additional protections be afforded [FN191] and the responsibilities and obligations of the Covered Entity in responding to such requests. Again, universities must develop policies concerning these requests and put mechanisms in place for agreeing to or denying the requests consistent with the requirements of the Privacy Regulations.

D. Issues of Special Concern to Universities

The Privacy Regulations implicate a number of areas that are unique, or of special concern, to universities. These include the impact of the Privacy Regulations on student clinical training, research, student health centers, fundraising and marketing.

1. Student Clinical Training

Universities that train future nurses, doctors, physical therapists, psychologists and other health care professionals often send their students to health care providers for clinical training. For instance, universities often send nursing students and medical students to hospitals or private practice facilities to obtain hands-on clinical training. While students are often supervised by personnel at the training site, universities sometimes send faculty members to the clinical site to provide supervision to the students. Although the Privacy Regulations are still in their infancy, there has already been a good deal of confusion about the relationship between, and the respective obligations of, the university and the

training facility under the Regulations. [FN192]

Contrary to what training sites might argue, universities that send students to facilities for clinical training generally are not business associates of those facilities. Importantly, in most cases, the university is not performing or assisting in the performance of a function or activity on behalf of the facility; the facility is actually assisting the university in the training of the university's students. Because universities are not business associates of the clinical facilities to which they send their students, they should resist efforts by hospitals ***560** and other health care training sites to require that the parties enter into business associate agreements. Because universities do not perform functions on behalf of training facilities when they send students for training, it is not appropriate for them to be defined as business associates and to accept the burdens and responsibilities that accompany that designation.

Under the Privacy Regulations, students who train at health care facilities -- and arguably the faculty members who are sent at times to supervise them -- are more appropriately considered part of the "workforce" of the facility. A Covered Entity's "workforce" includes "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." [FN193] Clearly, students are "trainees" whose work is "under the direct control" of employees of the health care facility to whom they are sent for training, and thus part of the training facility's "workforce." [FN194] Faculty members sent by a university to the health care training site to oversee the work of students are also arguably part of the site's workforce since they, too, generally work "under the direct control" of the site. Afterall, even the faculty supervisor works under the direction of the training facility's staff. Accordingly, for purposes of the Privacy Regulations, a university's students and faculty are part of the training facility's workforce; any requirements imposed by the Privacy Regulations with respect to those students and faculty rest with the facility, and as workforce members, those students and faculty will need to be trained in and comply with the training facility's HIPAA policies and procedures.

Although the Privacy Regulations may not place any affirmative obligations upon universities when they send students for training to clinical sites, it may nonetheless be in the best interests of universities -- not to mention within their education mission -- to train students in the requirements of HIPAA and the Privacy Regulations. Students who graduate from universities and enter health care professions anywhere in the country will necessarily confront the requirements of the Privacy Regulations in their day-to-day lives as health care professionals. Accordingly, as institutions that educate and train health care professionals, it may be advisable to add HIPAA and the Privacy Regulations to student curriculum. In addition, although health care training sites may not be able to require business associate contracts between themselves and universities, they could require as part of their affiliation agreements that universities train their students generally in the requirements of the Privacy Regulations.

***561** 2. Student Health Centers

The application of the Privacy Regulations to student health centers raises unique and complicated issues for some universities. Indeed, many questions have been raised among universities about the effect, if any, of the Privacy Regulations on student health centers, some of which treat only students and some of which treat a non-student population as well.

Initially, a university must determine whether its student health center is subject at all to the Privacy Regulations, i.e., does the student health center provide health care and engage in Electronic Transactions. [FN195] Because student health centers clearly provide health care, a university should focus on whether the student health center engages in Electronic Transactions. If the student health center does not engage in Electronic Transactions, then the health center is not subject to the Privacy Regulations.

If, on the other hand, a university determines that its student health center engages in Electronic Transactions, then the health center is covered under the Privacy Regulations. In large part, the extent to which the Privacy Regulations impact a covered student health center turns largely upon whether the health center treats non-students. Where a student health center treats only students, the student health records are either covered by FERPA or are exempt from FERPA. [FN196] In either case, all of the records are exempt from the Privacy Regulations since the records are excluded from the definition of PHI. [FN197] Accordingly, while the health center may technically be considered a covered component of the university under the Privacy Regulations, all of the individually identifiable health information it holds would be exempt from the application of the Regulations.

Where a covered student health center treats students as well as non-students such as faculty, staff or students' families, the identifiable health information of the non-student population is subject to the Privacy Regulations. In that case, the student health center faces difficult and complicated administrative issues since some of its health information (for students) is exempt from the Privacy Regulations, while other health information (for the non-student population) is not. Faced with this scenario, a student health center has a number of options. The health center can elect to treat the records of its students differently from the records of its non- student population, applying the policies and procedures required by the Privacy Regulations to the non-student population only. In practice, though, applying the requirements of the Regulations to only a subset of its patient- base will present difficult administrative burdens and may be simply unworkable. For instance, consider how a health center would implement different procedures for responding to requests for access to PHI based on the student-status of the patient.

***562** Alternatively, a student health center that treats non- students can elect to draft and implement HIPAA-compliant policies and procedures that apply to its entire patient population without regard to whether a particular patient is a student. In that way, the student health center's staff will need to learn only one set of policies and procedures that will apply uniformly to all patients of the health center, thereby easing the administrative burden. It should be noted, however, that while treating its patient population uniformly may be the only practical alternative for a university, by implementing policies and procedures for student records that are not legally required, a university unilaterally raises the standards against which its conduct will be judged. For instance, although a student who believes that the student health center has not acted in accordance with the Privacy Regulations cannot successfully argue that the health center has violated the Regulations with respect to that student's health information, the student can argue that the health center has violated its own policies and procedures.

Another option for the student health center is to treat all records as uniformly as possible in accordance with the obligations imposed by the Privacy Regulations. However, the student health center can identify those areas in which it is important that it not be bound by the Privacy Regulations with respect to student health records and modify its policies and procedures accordingly. For instance, a student health center can determine that it will use a HIPAA-compliant form of authorization for all releases of health information, whether for student or non-student health records. On the other hand, the health center can elect to exempt student records from the accounting requirements of the Privacy Regulations to the extent that complying with those requirements would be burdensome. Where a student health center elects to treat student and non-student records somewhat differently, the health center's Notice of Privacy Practices should reflect that decision. Indeed, the Notice should state, in any case, that the Privacy Regulations are not applicable to student health records and that those records will be treated by the health center in accordance with FERPA and the requirements of state law.

3. Research

Many researchers and research universities have expressed great concerns about the

effect of the Privacy Regulations on research which involves access to PHI. Many fear that what they see as the Regulations' burdensome requirements coupled with the possible sanctions for non-compliance will deter Covered Entities from providing access to PHI, thus adversely affecting the ability to conduct research. [FN198] While the effect of the Privacy Regulations on research remains to be seen, it is important that universities understand the ***563** requirements of the Regulations in the research arena so that they can comply with those requirements [FN199] and can confidently discuss the requirements with Covered Entities from which their researchers will need to obtain PHI.

a. Use or Disclosure for Research Pursuant to an Authorization

Access to PHI may always be granted to a researcher based on an authorization from the individual whose PHI is needed. [FN200] The rules regarding authorizations in the provider context [FN201] are generally applicable in the research area with a few important differences. First, contrary to the general rule that treatment may not be conditioned upon an individual's agreement to provide an authorization, health care providers "may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research ...." [FN202] Second, an authorization for use and disclosure of PHI for a research study "may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of [PHI] for such research or a consent to participate in such research." [FN203] Third, a research authorization does not need to contain an expiration date or event as is required for other authorizations; "[t]he statement 'end of the research study,' 'none,' or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository." ***564**[FN204] Accordingly, a university must prepare, and have available to its researchers, a distinct research authorization form (different from an authorization form it may use in the provider context) that meets the requirements of the Privacy Regulations. Because the research authorization may be combined with other documents related to a research study, such as consent to treatment, a university can start with the forms it is already using and modify them to include the language required by the Privacy Regulations with respect to research authorizations.

As is the case with authorizations generally, a research authorization may be revoked by an individual except to the extent that the Covered Entity has taken action in reliance on the authorization. [FN205] This rule raised concerns in the research community since the continued use of PHI collected prior to the revocation of authorization is often times vital to the overall research project. [FN206] As a result, although the language of the Privacy Rules was not changed, in August 2002 HHS clarified that the "reliance exception ... permits the continued use and disclosure of protected health information already obtained pursuant to a valid authorization to the extent necessary to preserve the integrity of the research study." [FN207]

b. Use or Disclosure for Research Not Requiring an Authorization

Absent individual authorization, the Privacy Regulations nonetheless permit access to PHI for research purposes in specific instances: pursuant to a waiver by an Institutional Review Board ("IRB") or Privacy Board, with respect to reviews preparatory to research, and with respect to review of decedent's information. [FN208] The requirements for access to PHI for reviews ***565** preparatory to research and with respect to the review of decedent's information are relatively straightforward. The Privacy Regulations generally require that the researcher provide the Covered Entity from whom PHI is sought with representations about the purposes for which the PHI will be used. [FN209]

The requirements of the Privacy Regulations concerning access to PHI pursuant to

an IRB or Privacy Board waiver are more complex and have created some anxiety in the research community. For universities with an already- existing IRB, the first decision that must be made is whether to use the IRB to review waiver requests or to establish a separate Privacy Board. [FN210] One advantage to using an existing IRB to consider waiver requests is that the body already exists and is familiar with many of the privacy issues regulated by the Privacy Regulations. However, depending on the volume of waiver requests anticipated and the existing workload of the IRB, it may not be practical to consider adding to the IRB's duties and responsibilities. Or, at the very least, a university may need to increase resources for the IRB if it decides to have the IRB be responsible for considering waivers. In addition, the IRB members will need training on the HIPAA regulations and related policies and procedures.

Alternatively, a university can create a Privacy Board to review and approve waivers. In order to integrate the waiver process into the existing IRB structure, the Privacy Board can be a designated subset of the IRB. Advantages of establishing a separate Privacy Board include the ability of universities to implement expedited review procedures. However, for those institutions that have difficulty finding people to serve on their IRBs, a separate Privacy Board may be all the more difficult to staff.

Once a university determines whether it will have its IRB or a separate Privacy Board be responsible for reviewing and approving waivers, the members of the IRB or Privacy Board must become familiar with the criteria pursuant to which they must analyze waiver requests. [FN211] These criteria include a determination that the use or disclosure of PHI presents "no more than a minimal risk to the [privacy of] individuals," [FN212] that the research cannot practically ***566** be done without the waiver, and that the research cannot practically be done without access to the PHI. [FN213] Although the waiver criteria were modified in August 2002 in response to concerns that the criteria were "confusing, redundant, and internally inconsistent," [FN214] there is still concern about interpreting the waiver criteria. To address these concerns, HHS intends to issue guidance documents; [FN215] hopefully, the guidance will be forthcoming and provide IRBs and Privacy Boards with some level of comfort that they are correctly interpreting and applying the criteria.

c. De-Identified Information and Limited Data Sets

Subsets of PHI may also be made available to researchers pursuant to the Privacy Regulations. For instance, De-Identified Information can be made available to researchers without a patient authorization. [FN216]

In addition, a limited data set may be made available for research purposes. [FN217] A limited data set is PHI that excludes certain direct identifiers of an individual or the individual's family, employer or household members including name, address other than town or city, state and zip code, telephone and fax numbers, social security number, account number and full face photographic images and any comparable images. [FN218] Unlike De-identified Information, a limited data set excludes less information from PHI, thus providing researchers with important information otherwise unavailable in De- identified Information.

In order to use or disclose a limited data set, a university (in its role as Covered Entity) must obtain "satisfactory assurance, in the form of a data use agreement ..., that the limited data set recipient will only use or disclose the protected health information for limited purposes." [FN219] A data use agreement must contain specific provisions required by the Privacy Regulations, ***567** including (1) a statement of the permitted uses and disclosures of the limited data set by the recipient, (2) the identification of those who are permitted to use or receive the limited data set, and (3) a provision stating that the recipient will, inter alia, use safeguards to prevent use or disclosure of information other than as permitted pursuant to the data use agreement, report unauthorized uses or disclosures, and not identify the information or contact the individuals. [FN220] Universities that are covered health care providers should have a standard form data use agreement available to use in those instances in which it releases a limited data set for

research purposes. In addition, researchers should be familiar with the contents of data use agreements since they may be asked to sign them.

4. Fundraising and Marketing

Universities that use PHI to conduct fundraising or marketing will need to review their practices to ensure that they comply with the Privacy Regulations, which address both areas.

a. Fundraising

Fundraising is important to the life of universities, including those with medical and dental schools or those that are part of a large academic medical center. In the case of universities that include health care providers, PHI has sometimes been used in connection with their fundraising efforts. As such, those universities will now be required to conduct such fundraising in accordance with the Privacy Regulations.

Despite the importance of fundraising to universities, the Privacy Regulations and commentary say little about the use of PHI for fundraising and the practical impact that the Regulations will have on fundraising practices. In fact, the Privacy Regulations raise many more questions than they resolve about the permitted uses and disclosures of PHI for fundraising purposes.

Basically, the Privacy Regulations allow a university to use or disclose to a business associate or institutionally related foundation, an individual's demographic information [FN221] and dates of health care service "for the purpose of raising funds for its own benefit ...." [FN222] Universities may not without a patient's authorization use an individual's diagnosis to target that person for fundraising. A hospital, for instance, cannot direct literature requesting money to build a new cancer center only to patients who have been treated for cancer. The Privacy Regulations say nothing further about fundraising; in fact, the Regulations do not even contain a definition of "fundraising."

***568** While the fundraising requirements may appear to be clear, they may be problematic for universities that are complex or that have close and symbiotic relationships with other institutions such as hospitals. The following are a couple of examples that may illustrate the dilemma faced by some universities:

* An academic medical center has many different departments or administrative units that operate autonomously for purposes of the care each provides but are not separately incorporated. Assume that one of the units is a large cancer center that has a large staff and treats thousands of patients. In the past, the center -- through the university's development staff -- has helped to support its work through fundraising efforts directed at its patients. Absent an authorization signed by a patient, the Privacy Regulations appear to call that practice into question since the university would be arguably using the patients' diagnosis (i.e., cancer) to appeal to those individuals to support the cancer center. Making that outcome more absurd is the fact that the center could engage in such fundraising if it were a separate covered entity. Unfortunately, the Privacy Regulations do not take into account the reality of the situation: patients who are treated at a university's cancer center may actually feel more ties to the center than to the university, in the abstract, and may be more likely to support the work of the department of the university to which they feel more connected.

* An academic medical center has an extremely close relationship with a hospital, to which it is also physically close. For the most part, the medical school's physicians are the "doctors" at the hospital and the hospital and school may share services. In fact, patients -- and even employees -- may not always recognize that the school and hospital are separate corporate entities. In the past, the hospital has supplied patient information -- information about patients seen by medical school doctors working at the hospital -- to the school for purposes of development. Absent an authorization by an individual, the Privacy Regulations may call this practice into doubt because the hospital may use a patient's demographic

information only for purposes of fundraising for its own benefit.

For some universities, then, it may be difficult to determine whether, and to what extent, its fundraising practices need to be modified to comply with the Privacy Regulations -- an analysis made all the more critical in light of the impact the determination could have on a university's ability to raise much-needed funds. Whatever its current fundraising practices, however, there are certain things that universities can do. First, a university can always consider obtaining an authorization from each individual to whom services are provided that specifically permits the university to send the individual fundraising literature, including fundraising which is based on, or related to, that individual's diagnosis. A university that goes this route must be diligent ***569** about sending fundraising literature not otherwise permitted by the Privacy Regulations to only those individuals who have provided an authorization. In addition, a university that relies on authorizations must make sure that the authorization contains an expiration date [FN223] and that a mechanism is put in place to ensure that fundraising literature is not sent to an individual after the individual's authorization has expired, [FN224] or has been revoked. [FN225] One can imagine that this may be difficult and burdensome for a university to do.

For universities that elect not to obtain authorizations, there may be some practices to emphasize that do not appear to run afoul of the Privacy Regulations. For instance, a university may consider a system for categorizing individuals according to the donations made by those individuals so that future fundraising literature may be directed to those individuals in accordance with their demonstrated interest. For example, a university could legitimately direct fundraising literature requesting funds for a cancer research project to individuals who have contributed in the past to its cancer center or other cancer projects; the university would be directing fundraising materials to individuals based on those individuals' demonstrated interests rather than on PHI. [FN226]

For those universities that use patient information for fundraising, there are other administrative obligations that must be met. For instance, if the university intends to use PHI for fundraising, its Notice of Privacy Practices must say so. [FN227] In addition, all fundraising literature sent to individuals must include a mechanism allowing the individual to opt-out of receiving future fundraising material, and the university must make reasonable efforts to ensure that an individual who opts-out receives no further fundraising material. [FN228] The manner in which a university will accomplish this will depend upon the systems the university already has in place for fundraising. A university that fundraises using a database of names may consider instituting a mechanism for insuring that names are deleted from the database.

b. Marketing

Pursuant to the Privacy Regulations, "marketing" includes any communication made about a product or service that encourages another person to use or buy the product or service. [FN229] An example of a marketing activity is ***570** when a Covered Entity provides a drug manufacturer with a list of patients for which the manufacturer pays the Covered Entity and then uses that list to send discount coupons for a new drug directly to the patients. [FN230] Marketing, however, does not include communications made for an individual's treatment, for an individual's case management or care coordination, to recommend alternative treatments or therapies, or that is intended to describe a health product or service provided by the Covered Entity. [FN231] So, for instance, it is not considered marketing when a pharmacy mails prescription refill reminders to patients. [FN232]

Generally, a university must obtain an authorization from an individual in order to engage in marketing with that person unless the communication is a face-to-face communication or involves a promotional gift of nominal value. [FN233] An authorization would not be required, then, when a hospital provides free infant formula samples and baby products to new parents leaving the hospital. [FN234]

Again, universities should formulate and implement policies and procedures that set forth the requirements of the Privacy Regulations as they relate to marketing activities.

III. THE PRIVACY REGULATIONS: THE UNIVERSITY AS GROUP HEALTH PLAN SPONSOR

Separate and apart from whether a university must comply with the Privacy Regulations because it provides health care services, many universities will be affected by the Privacy Regulations to the extent that they offer health plan benefits to employees since health plans are Covered Entities under the Regulations. [FN235] A "health plan" under the Privacy Regulations is "an individual or group plan that provides, or pays the cost of, medical care" and includes, inter alia, both insured and self-insured group health plans. [FN236] The Privacy Regulations, like ERISA, treat a covered group health plan as a separate entity. Accordingly, for universities that offer group health plans, it is important to note that the plans are not part of the university's covered components for purposes of the Privacy Regulations, but rather, are separate HIPAA Covered Entities. [FN237]

***571** A. Health Plans Covered by the Privacy Regulations and How To Identify Them

Initially, a university will need to inventory the health benefits it offers and determine which benefits are subject to the Privacy Regulations. For instance, to the extent that a university maintains group health, vision, dental, prescription drug and long-term care plans, those plans would be subject to the Privacy Regulations since they fall within the definition of a "health plan." [FN238] Other plans, such as disability, liability and workers' compensation plans, are specifically excluded from the definition of "health plan" under the Privacy Regulations and, thus, would not be covered by the Regulations. [FN239] Still other plans, such as life and retirement plans, are not health plans covered by the Privacy Regulations because they do not "provide[,] or pay[] for the cost of[,] medical care." [FN240] Finally, a university should identify any Section 125 cafeteria plan or flexible spending account it offers. "Cafeteria plans typically permit participants to apply portions of their compensation toward different plans offered by their employer." [FN241] Because the benefits in a cafeteria plan are paid by underlying plans, the cafeteria plan itself does not provide or pay the cost of medical care and, therefore, is not likely covered by the Privacy Regulations. [FN242] On the other hand, flexible spending accounts generally cover costs not paid for by other plans. Because those accounts do provide or pay the cost of medical care, they are likely covered by the Privacy Regulations. [FN243]

Once a university inventories its health plans and determines which plans are covered by the Privacy Regulations, it should identify which of its plans are self-funded and which are fully-insured. Moreover, for those fully- insured plans, the university should determine whether it receives any PHI in connection with the plans. These determinations are important because a university's obligations under the Privacy Regulations -- and consequently, its compliance burdens -- differ considerably depending on whether its plans are self-funded [FN244] or fully insured. [FN245]

Finally, a university needs to determine whether its plans should be identified as separate plans based on its contracts with providers or based on what might be included on an ERISA filing.

***572** A preliminary inquiry having received little scholarship is what is the group health plan for Privacy Rule purposes? Assuming for instance that ... the health benefits are provided through three different provider networks according to three different "plans" ..., all of which are filed within a single ERISA Form 5500, are there three separate group health plans based on the contracts with the three types of providers, or a single group health plan given the single ERISA filing? If each of these health benefit plans is a single group health plan for Privacy Rule purposes because each provides medical care to over 50 participants, then each plan will theoretically be required to independently comply with HIPAA, including

compliance with the notice and administrative requirements where applicable depending on whether the plan is self-funded or fully insured. However, if the ERISA filing is used to define the legal parameters of the group health plan, then a single notice of privacy practices and a single set of policies and procedures could be used for all three benefit plans as together these plans would comprise a single group health plan. [FN246]

A university should also consider whether its separate plans -- however defined -- should enter into an OHCA in order to minimize the administrative burdens of the Privacy Regulations on the plans. [FN247] Pursuant to the Privacy Regulations, group health plans that are maintained by the same plan sponsor, or group health plans and a health insurance issuer or HMO with respect to PHI "created or received by such health insurance issuers or HMOs that relates to individuals who are or who have been participants or beneficiaries in any such group health plan," may enter into an OHCA. [FN248] As such, the group health plans that participate in an OHCA may issue a single Notice of Privacy Practices and otherwise undertake joint actions to comply with the Privacy Regulations.

B. Sharing of Information between the Group Health Plan and Plan Sponsor

The Privacy Regulations set forth the circumstances under which PHI can be shared between the group health plan and the university as plan sponsor. Generally, there are three broad categories of PHI that can be shared between a group health plan and the plan sponsor: (a) De-identified Information, [FN249] (b) summary health information requested by the plan sponsor to ***573** obtain premium bids or to modify, amend, or terminate the group health plan, [FN250] and (c) enrollment or disenrollment information. [FN251]

In addition, the group health plan may disclose PHI to the plan sponsor "to carry out plan administration functions that the plan sponsor performs" so long as the group health plan's plan documents have been amended to incorporate those provisions required by the Privacy Regulations, including the permitted and required uses and disclosures of PHI by the plan sponsor and representations by the plan sponsor about how it will safeguard the information. [FN252] A group health plan may not share PHI with the plan sponsor until the plan sponsor provides it with a certification that the plan documents have been amended as required by the Privacy Regulations. [FN253] Accordingly, a university should evaluate the kind of information it currently receives from its health plan and amend its plan documents as necessary in order to ensure that the required information can continue to be provided. [FN254]

C. Administrative Requirements

Covered health plans under the Privacy Regulations are required to assume many of the same kinds of administrative responsibilities as covered health care providers. [FN255] For instance, a covered health plan must provide a Notice of Privacy Practices to all plan members, be prepared to account for certain uses and disclosures of PHI and enter into business associate agreements with third parties performing services on behalf of the plan which involve access to the plan's PHI. The extent to which a university, as health plan sponsor, is responsible for undertaking these administrative responsibilities depends upon whether its health plans are self-funded or fully-insured and, if fully-insured, on the extent to which the university may receive PHI in connection with the plan.

1. Self-funded Plans

Where one or more of a university's health plans are self-funded, the university as plan sponsor will be responsible for many of the administrative obligations imposed by the Privacy Regulations and should have policies and procedures in place with respect to the permitted uses and disclosures of PHI held by the plans.

***574** Customarily, a self-funded health plan is administered by a third party administrator that handles the day-to-day plan administration activities. Because third-party administrators perform functions on behalf of a covered health plan, a university must ensure that there is a business associate agreement in place between each plan and its third-party administrator. [FN256] Because the health plan is not otherwise a separate corporate entity, the agreement can be entered into by the university as employer sponsor on behalf of the plan.

Moreover, as sponsor of a self-funded plan, a university must provide to plan members a Notice of Privacy Practices on behalf of each self-insured health plan or OHCA. [FN257] Generally, the Notice of Privacy Practices for a health plan must contain the same kinds of information contained in a Notice provided by a health care provider including examples of the uses and disclosures of PHI that the health plan will engage in and a statement about the individual's right to amend PHI, access PHI and receive an accounting of the plan's uses and disclosures of PHI. [FN258]

A university should also designate a privacy official for its health plans or OHCA. [FN259] Again, the role of the privacy official will be similar to the role of the privacy official designated for a health care provider. [FN260] A university must also put into place policies and procedures with respect to an individual's rights under the Privacy Regulations including access to PHI, [FN261] accounting of disclosures, [FN262] requests for amendment of PHI, [FN263] and requests for additional privacy protections. [FN264] Finally, a university should put into place policies and procedures to ensure that those involved in the administration of the health plan use or disclose only the minimum necessary PHI to carry out the purpose of the use or disclosure. [FN265]

***575** 2. Fully-insured Plans

Universities face fewer compliance burdens with respect to their insured plans since the HMO or insurer vendor handles most covered functions and PHI. [FN266]

> Fully insured group health plans that do not create or receive PHI (although they may receive summary health information and/or enrollment or disenrollment information) are not required to develop a notice of privacy practices, nor are they subject to the most burdensome administrative requirements of the Privacy Rule, including the training and policies/procedures requirements ... Such group health plans must nevertheless still document the fact that their plan documents have been amended as required by the Rule, and must also abide by the administrative standards which prohibit intimidating and retaliatory acts and which forbid the relinquishment of rights bestowed under the Rule. [FN267]

Fully-insured plans that create or receive PHI have additional burdens.

> The obligations of these group health plans are less onerous than those of self-funded plans because unlike self-funded plans which must both develop and distribute a notice of privacy practices to all of their enrollees, fully insured plans that create or receive PHI are required to maintain a notice of privacy practices, but are under no obligation to distribute it to enrollees (unless an express request for a notice is made by a particular enrollee in which case a notice must be provided to that enrollee). [FN268]

Fully-insured plans that create or receive PHI must also amend their plan documents as required by the Privacy Regulations and comply with the Regulations' other administrative requirements.

IV. A UNIVERSITY'S TRAINING OBLIGATIONS

The Privacy Regulations require a university to train each member of its workforce within the covered component(s) of the university, and thereafter each new member of its workforce, on its policies and procedures with respect to PHI necessary and appropriate for the members of the workforce to carry out their jobs. [FN269] When

there is a material change in a HIPAA policy or procedure, the university must re-train those members of its workforce affected ***576** by the modified policy or procedure. [FN270] Finally, a university is required to document the training of its workforce. [FN271]

Accordingly, once a university has drafted its policies and procedures, it must undertake to train the employees in its covered components with respect to those policies and procedures. Depending on the extent of a university's health care operations and health insurance products, the training obligation can be overwhelming, covering diverse operations and affecting many employees. [FN272] For instance, contemplate the training obligations for a university which has a large staff to help administer a number of employee health plans, runs a student health center which treats a non-student population, operates a dental school with clinics, operates a medical school which also includes the provision of health care by faculty practice groups, is a research institution with many researchers who require access to PHI and has units around the university which provide support functions to those operations. Under the Privacy Regulations, the university must train all of its employees who work in these areas on the distinct and unique HIPAA policies and procedures that are in place in the respective units.

Because the Privacy Regulations affect health care providers and health plans of all sizes, the Privacy Regulations do not mandate one particular type of training method for Covered Entities. Rather, the Privacy Regulations are intended to allow Covered Entities the flexibility to formulate policies, procedures and training programs "tailored to fit their size and needs." [FN273] For instance, "[t]he training requirement may be satisfied by a small physician practice's providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies; whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs." [FN274]

Accordingly, each university must assess its training needs in light of the size and type of its covered health care operations and its health plans. What is sufficient for one university may not necessarily work for another university. A university might consider offering a single type of training or combining different training methods. For instance, a university can offer "live" training, where a person well-versed in the Privacy Regulations and the university's policies and procedures can present training to a group or groups of the university's affected staff. A university might consider taping such live training sessions and replaying them for staff as needed. A university could even consider putting such taped sessions on its website, where its employees could then have access to it. In addition to these live sessions, a university could also consider offering training through a web-based training module that it either designs or purchases from a third-party vendor. Whatever training ***577** method a university chooses, the university should make and maintain a record of attendees. The training should also be such that it can be easily delivered to new staff members on a rolling basis.

V. THE CONSEQUENCES OF NONCOMPLIANCE WITH THE PRIVACY REGULATIONS

As previously discussed, universities are required to designate a person or office "who is responsible for receiving complaints" about a university's alleged noncompliance with the Privacy Regulations. [FN275] Once a university designates a person or office responsible for receiving complaints, the university must develop a process for handling any complaints that are made. [FN276] If a university determines, either in response to a complaint or on its own, that an employee has failed to comply with the Privacy Regulations or its HIPAA policies and procedures, then the university must sanction the employee in accordance with established policies. [FN277] The university must document any sanctions that it applies. [FN278]

In addition to filing a complaint with the university, an individual is also free to file a complaint with HHS. [FN279] HHS has delegated enforcement of civil compliance to the Office for Civil Rights (OCR). [FN280] For its part, OCR can

investigate complaints filed, which may include "review of the pertinent policies, procedures, or practices" of the university and "of the circumstances regarding any alleged acts or omissions concerning compliance." [FN281] OCR also has the authority to conduct compliance reviews on its own. [FN282]

Depending on the nature of the violation, universities may be subject to civil and/or criminal penalties for violations of the Privacy Regulations. [FN283] In general, HHS may impose a penalty up to $100 for each violation of the Privacy Regulations, not to exceed $25,000 during any calendar year. [FN284] If a ***578** person knowingly obtains or discloses someone's PHI, then the possible penalties are greater, including the imposition of a fine of up to $50,000 and a year in prison, or both. [FN285] For those violations committed "with intent to sell, transfer, or use" PHI "for commercial advantage, personal gain, or malicious harm," violators face fines of up to $250,000 and up to ten years in prison, or both. [FN286]

VI. CONCLUSION

The Privacy Regulations embody a complex regulatory scheme that sets forth a plethora of obligations, requirements and potential pitfalls. Navigating the Privacy Regulations presents a major challenge for universities and their counsel. As universities undertake the challenge, they should be diligent and take reasonable steps to ensure that they meet their many compliance burdens under the Regulations.

[FNa1]. Associate General Counsel, New York University. B.A., New York University, 1983; J.D., New York University School of Law, 1986. The author would like to thank Marie Pollio, a second-year law student at New York University School of Law, for her invaluable assistance with this article.

Due to the potential for revision of the Code of Federal Regulations ("C.F.R.") in connection with the implementation of regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the delay caused by publication, all citations to the C.F.R. are current as of April 14, 2003.

[FN1]. For purposes of this article, references to "university" will include colleges.

[FN2]. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 264 (1996), 110 Stat. 1936, 2033 (codified at 42 U.S.C. § 1320d-2(note) (2000)); Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160 (2002), 45 C.F.R. § 164 subpts. A, E (2002).

[FN3]. That very real concern arose out of the common practice of excluding coverage, either for a specified period of time or permanently, for "pre- existing conditions," which were medical conditions that the employee or employee's dependent experienced prior to signing onto a new health insurance program. H.R. Rep. No. 104-496, at 68 (1996), reprinted in 1996 U.S.C.C.A.N. 1865, 1868.

[FN4]. See 29 U.S.C. § § 1181-1183 (2000).

[FN5]. H.R. Rep. No. 104-496, at 67 (1996), reprinted in 1996 U.S.C.C.A.N. at 1866. This aim included administrative simplification "by encouraging the development of a health care network through the establishment of standards and requirements for the electronic transmission of certain health information." Id.

[FN6]. Id.

[FN7]. Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (1996).

[FN8]. Pub. L. No. 104-191, § 264(c)(1), 110 Stat. 1936, 2033 (1996).

[FN9]. Pub. L. No. 104-191, § 264(b), 110 Stat. 1936, 2033 (1996).

[FN10]. H.R. Rep. No. 104-496 and H.R. Conf. Rep. No. 104-191 (1996), reprinted in 1996 U.S.C.C.A.N. 1990.

[FN11]. H.R. Rep. No. 104-496, at 100 (1996), reprinted in 1996 U.S.C.C.A.N at 1900. The house conference report contains similar language concerning the protection of patient information. H.R. Conf. Rep. No. 104- 191, at 265 (1996), reprinted in 1996 U.S.C.C.A.N at 2078.

[FN12]. 45 C.F.R. § 160, 164 (2002). Regulations were also promulgated requiring the standardization of electronic transactions and code sets. Health Insurance Reform: Standards for Electronic Transactions, 45 C.F.R. § § 160, 162 (2002); Health Insurance Reform: Modifications to Electronic Data Transaction Standards and Code Sets, 68 Fed. Reg. 8,381, 8,383 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 162). Entities were required to comply with those regulations by October 16, 2002, although many entities took advantage of a one-year extension of the compliance date established by Congress pursuant to the Administrative Simplification Compliance Act. 42 U.S.C. § 1320d- 4(note) (2002). Entities that wanted the extension were required to file an application with HHS by October 16, 2002. Id. See also 45 C.F.R. § § 162.900, 162.940 (2002). Finally, regulations have been published concerning the security of health information. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, & 164). Entities are required to comply with the security regulations by April 21, 2005. Id.

[FN13]. See 45 C.F.R. § § 160, 164 (2002). The modifications to the privacy regulations published in August 2002 ("August 2002 Modifications") made some significant changes to the Regulations as originally promulgated. For instance, the August 2002 Modifications omitted the requirement that providers obtain the written consent of patients to use and disclose patient health information for treatment, payment and health care operations. Id. The August 2002 Modifications also modified the law in other areas affected by the Regulations including incidental disclosures, marketing, authorization forms, research, and accountings. Id.

[FN14]. 45 C.F.R. § 164.524 (2002). Small health plans, which are plans with annual receipts of five million dollars or less, have until April 14, 2004, to comply with the Privacy Regulations. 45 C.F.R. § 164.524(b)(2) (2002). The Privacy Regulations survived a legal challenge brought by the Association of American Physicians & Surgeons, Inc. who argued that by including non-electronic health information, the Regulations went beyond the legislative scope of HIPAA, and that by interfering with private communications between doctors and patients the statute violated the First, Fourth and Tenth Amendments. Ass'n of Am. Physicians & Surgeons, Inc. v. U.S. Dept. of Health & Human Servs., 224 F.Supp. 2d 1115, 1129 (S.D. Tex. 2002) (dismissing the claim that the regulations went beyond the scope of HIPAA claim because the statutory language contemplated regulation beyond mere electronically transmitted data and dismissing the constitutional claims because of lack of standing to sue and lack of ripeness). The court also rejected arguments that the regulations violated the Paperwork Reduction Act and Regulatory Flexibility Act. Id. at 1128-29.

[FN15]. Where an entity engages in activities in addition to the delivery of health services covered by the Privacy Regulations, the Regulations permit the entity to declare itself a "hybrid entity." 45 C.F.R. § 164.504(a) (2002). For a more detailed discussion of if and how a university can declare itself a hybrid entity, see infra Part II.A.1.

[FN16]. 45 C.F.R. § 164.530(i)(1) (2002). Moreover, the "policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance." Id.

[FN17]. 45 C.F.R. § 164.530 (2002).

[FN18]. 45 C.F.R. § 164.530(b) (2002).

[FN19]. 45 C.F.R. § 160.103 (2002) (defining "Covered Entity").

[FN20]. 45 C.F.R. § 160.102(a) (2002).

[FN21]. "[']Transaction['] means 'the transmission of information between two parties to carry out financial or administrative activities related to health care ... [including] ... (1) [h]ealth care claims or equivalent encounter information[;] (2) [h]ealth care payment and remittance advice [;] (3) [c]oordination of benefits[;] (4) [h]ealth care claim status[;] (5) [e]nrollment and disenrollment in a health plan[;] (6) [e]ligibility for a health plan[;] (7) [h]ealth plan premium payments[;] (8) [r]eferral certification and authorization[;] (9) [f]irst report of injury[;] (10) [h]ealth claims attachments[; and] (11) [o]ther transactions that the Secretary may prescribe by regulation."' 45 C.F.R. § 160.103 (2002) (emphasis omitted).

[FN22]. HHS has created decision-making tools to help organizations determine whether they are Covered Entities. See Centers for Medicare & Medicaid Services, Covered Entity Decision Tools, available at http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decision-support/default.asp (last visited Apr. 14, 2003). Universities may also provide employee or student health benefits through group health plans and other arrangements that qualify as HIPAA-covered health plans. Universities' HIPAA obligations with respect to covered health plans are discussed infra Part III.

[FN23]. Those areas of a university that provide support services to a provider covered by the Privacy Regulations should be identified so that it can be determined whether or not to include those support areas as part of the university's Covered Entity. For a more detailed discussion about how a university designates its components covered by the Privacy Regulations, see infra Part II.A.1. As will be discussed, whether or not a department, unit or school is considered part of a university's Covered Entity will affect the ability of that department, unit or school to receive Protected Health Information from the university's covered components.

[FN24]. The presence of one or more health plans at a university does not factor into this analysis. As will be discussed more fully in infra Part III, under the Privacy Regulations each health plan is its own separate Covered Entity.

Accordingly, to the extent that a university has HIPAA-covered health plans, those plans are not part of the university as a Covered Entity, but rather are each their own HIPAA Covered Entities.

[FN25]. 45 C.F.R. § 164.504(a) (2002). This provision was changed to its current form in August 2002. Formerly, the Regulations defined hybrid entities as those Covered Entities whose "primary" activities were those not covered by the Privacy Regulations. The August 2002 Modifications removed the term "primary" from the definition of hybrid entities and gave entities covered by the Regulations the discretion to determine whether they wanted to be designated hybrid entities. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,205 (Aug. 14, 2002) (codified at 45 C.F.R. § § 160, 164 (2002)).

[FN26]. 45 C.F.R. § 164.504(b) (2002).

[FN27]. The training required by the Privacy Regulations will be addressed infra Part IV.

[FN28]. Section 164.504(c)(3)(i) makes clear that the entity, in this case the university, is ultimately responsible for compliance by its component(s). 45 C.F.R. § 164.504(c)(3)(i) (2002).

[FN29]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,205.

[FN30]. "Transfer of protected health information held by the health care component to other components of the hybrid entity continues to be a disclosure under the Privacy Rule, and, thus, allowed only to the same extent such a disclosure is permitted to a separate entity." Id.

[FN31]. A university can elect to declare an entire school a covered component or only those parts of a school that provide HIPAA-covered health services. For instance, a university could elect to treat its medical school as a covered component but except out of that designation the school's student health services or other departments which do not engage in Electronic Transactions. As discussed above, while a university is permitted to do this, it may also determine that this approach is not practical.

[FN32]. In addition to designating as part of its health care component those components which perform health care functions, the Privacy Regulations permit a Covered Entity to include a component "only to the extent that it performs: (A) Covered functions; or (B) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities." 45 C.F.R. § 164.504(c)(3)(iii) (2002).

[FN33]. 45 C.F.R. § 164.508 (2002). The authorization requirements under the Privacy Regulations are discussed infra Part II.B.2.c.

[FN34]. Although a Covered Entity is not required under the Privacy Regulations to designate as part of the Covered Entity those components that perform "business associate"-type functions, not including such components restricts the free flow of patient-specific health information to those areas.

[A] disclosure of protected health information from the health care component to such other division that is not part of the health care component is the same as a disclosure outside the covered entity. Because an entity cannot have a business associate contract with itself, such a disclosure likely will require individual authorization.
Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,205. Requiring an authorization for the release of health information from a covered component of a university to another area of the university that provides business-associate functions to the covered component would create administrative problems for many universities.

[FN35]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,205.

[FN36]. 45 C.F.R. § § 164.504(c)(3)(iii), 164.530(j) (2002).

[FN37]. For instance, a clinic that does not currently engage in Electronic Transactions, and thus may not be identified as a covered component of the university's hybrid entity, may decide to engage in such transactions in the future. When the clinic engages in Electronic Transactions, it will become a covered component of the hybrid entity subject to the Privacy Regulations. Indeed, a university should consider instituting some mechanism for confirming its covered components, possibly on an annual basis.

[FN38]. This discussion will focus on organized health care arrangements in the context of the provision of health care. It should be noted that OHCAs may also exist with respect to covered health plans. That issue will be discussed infra Part III.A.

[FN39]. 45 C.F.R. § 164.501 (2002).

[FN40]. Id.

[FN41]. Id. Specifically, this includes utilization review "in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf." Id.

[FN42]. Id. Specifically, this includes quality assessment and improvement activities "in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf." Id.

[FN43]. Id. Specifically, this includes payment activities "if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk." Id.

[FN44]. 45 C.F.R. § 164.520(d) (2002). It should be noted that, as will be discussed infra Part II.C.2., the Privacy Regulations require Covered Entities to provide a notice of privacy practices to patients on their first encounter with a

health care provider. The notice of privacy practices sets forth, inter alia, the ways in which protected health information is used and disclosed by the Covered Entity. 45 C.F.R. § 164.520(b) (2002). In the case of notices provided by members of an OHCA, there are certain additional requirements. 45 C.F.R. § 164.520(d). Moreover, although true compliance as a single entity can only occur for an affiliated covered entity, OHCA participants, although separate for compliance purposes, can share a joint Notice of Privacy Practices and share PHI for joint operations.

[FN45]. At this point, it is not clear whether and to what extent participants in an OHCA become jointly liable for violations of the Privacy Regulations. Given that the OHCA participants may rely on each other in some way to fulfill their respective obligations under the Regulations and share PHI for certain joint operations, it may be that they will also be held jointly accountable should either or both fail to comply with the Regulations with respect to the OHCA.

[FN46]. 45 C.F.R. § 164.520(d)(1) (2002).

[FN47]. 45 C.F.R. § 164.502(a) (2002). When analyzing its obligations under the Privacy Regulations, universities must also consider the application of state law. See 45 C.F.R. § § 160.201-160.205 (2002), which concern the interaction of the Privacy Regulations and state law and set forth the circumstances under which the Privacy Regulations pre-empt state law. In general, if state law has more stringent requirements with respect to PHI, then state law will control. 45 C.F.R. § 160.203(b) (2002). Accordingly, when developing their HIPAA policies and procedures, universities must always be aware of the requirements of state law that may be applicable to a particular policy or procedure contemplated, and the policy or procedure must reflect those state law requirements where applicable. For a helpful discussion on HIPAA preemption, see Mark Barnes et al., The HIPAA Privacy Rule: A Guide to Conducting State Law Preemption Analyses, 11 BUREAU OF NAT'L AFF. HEALTH L. REP. (2002).

[FN48]. 45 C.F.R. § 164.501 (2002) defines "Protected Health Information" as all individually identifiable health information except as specifically provided in the Privacy Regulations.

[FN49]. 45 C.F.R. § 160.103 (2002).

[FN50]. 45 C.F.R. § 164.501 (2002). In the original Privacy Regulations, PHI was defined broadly to include all PHI "maintained or transmitted by a covered entity in any form or medium." Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,191. However, "throughout the ... preamble to the Privacy Rule, [HHS] repeatedly stated that the Privacy Rule does not apply to employers, nor does it apply to the employment functions of covered entities, that is, when they are acting in their role as employers." Id. Because of the confusion created by the seeming conflict between the plain language of the Privacy Regulations and the commentary provided by HHS, the Privacy Regulations were modified in August 2002 to specifically exclude from the definition of PHI "employment records" held by Covered Entities. 45 C.F.R. § 164.501 (2002). HHS cautions, however, that "a covered entity must remain cognizant of its dual roles as an employer and as a health care provider, health plan, or health care clearinghouse." Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,192.

[FN51]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,192.

[FN52]. Of course, this is not to suggest that a university should not otherwise protect the confidentiality of this information. However, the use and disclosure of the information is not subject to the myriad requirements of the Privacy Regulations.

[FN53]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,192.

[FN54]. 20 U.S.C. § 1232g (2000).

[FN55]. The records that FERPA excludes relate to records on a student who is eighteen or older, attending an institution of postsecondary education (an "eligible student"), that are: "made or maintained by a ... recognized [medical] professional ... acting in his professional ... capacity, ... and which are made, maintained, or used only in connection with the provision of treatment to the student," and disclosed only to individuals providing treatment, "except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice." 20 U.S.C. § 1232g(a)(4)(b)(iv) (2000).

[FN56]. 45 C.F.R. § 164.501 (2002).

[FN57]. A more detailed discussion of the interaction between FERPA and HIPAA in the context of student health centers will be discussed infra Part II.D.2.

[FN58]. 45 C.F.R. § 164.514(a) (2002).

[FN59]. 45 C.F.R. § 164.502(d)(2) (2002).

[FN60]. 45 C.F.R. § 1564.514(b)(1) (2002).

[FN61]. 45 C.F.R. § 164.514(b)(1)(i) (2002). In addition, that determination must be documented. 45 C.F.R. § 164.514(b)(1)(ii) (2002).

[FN62]. 45 C.F.R. § 164.514(b)(2) (2002), which includes a list of the eighteen specific identifiers. The Privacy Regulations also permit a Covered Entity to "assign a code or other means of record identification" to De- identified Information so that the information can be re-identified at a later time. 45 C.F.R. § 164.514(c) (2002). Of course, once De-identified Information is re-identified, it is PHI subject to the Privacy Regulations. 45 C.F.R. § 164.502(d)(2)(ii) (2002).

[FN63]. 45 C.F.R. § 164.514(b)(2)(ii) (2002).

[FN64]. Universities may also send students to clinical sites for training. Universities should be aware that while students, in the past, may have brought patient information back to the university to be used as part of their educational training, hospitals and other health care sites likely will not permit that practice to continue.

[FN65]. 45 C.F.R. § 164.530(i)(1) (2002). With respect to permissive uses and disclosures of PHI, the Privacy Regulations provide "a Federal floor of privacy protections for individuals"' health information. United States Department of Health & Human Services Questions & Answers, Does the HIPAA Privacy Rule preempt State Laws?, at http://www.hhs.gov/ocr/hipaa/ (last visited Apr. 23, 2003) [hereinafter "HHS FAQs"] (to retrieve this citation access the link entitled "View Health Information Privacy Frequently Asked Questions (FAQs)," then enter the question in the Search Text box). A Covered Entity may elect, in certain instances, to institute policies and procedures that are more restrictive than the requirements of the Privacy Regulations.

[FN66]. 45 C.F.R. § 164.530(i)(1) (2002).

[FN67]. See 45 C.F.R. § § 164.502(a)(2)(i), 164.524 (2002), which will be discussed further infra Part II.C.3.

[FN68]. See 45 C.F.R. § § 164.502(a)(2)(i), 164.528 (2002), which will be discussed further infra Part II.C.4.

[FN69]. 45 C.F.R. § 164.502(a)(2)(ii) (2002).

[FN70]. 45 C.F.R. § 164.502(a)(1)(ii) (2002). "Treatment" is defined under the Privacy Regulations as "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another." 45 C.F.R. § 164.501 (2002). For instance, a health care provider may use PHI to consult with another provider for the purposes of treating a patient. OFFICE OF CIVIL RIGHTS, DEPT. OF HEALTH AND HUMAN SERVICES, GUIDANCE EXPLAINING SIGNIFICANT ASPECTS OF THE PRIVACY RULE 56, 20 & 22 (Apr. 3, 2002), available at http://www.hhs.gov/ocr/hipaa/privacy.html [hereinafter "GUIDANCE"]. It is important to note that special rules apply to the use and disclosure of psychotherapy notes, even if the use or disclosure is for the treatment of the individual. 45 C.F.R. § 164.508(a)(2) (2002).

[FN71]. 45 C.F.R. § 164.502(a)(1)(ii) (2002). "Payment" is defined under the Privacy Regulations as, inter alia, activities undertaken by a health care provider "to obtain or provide reimbursement for the provision of health care," including billing, claims management, collection activities, utilization review activities and certain reporting to consumer reporting agencies. 45 C.F.R. § 164.501.

[FN72]. 45 C.F.R. § 164.502(a)(1)(ii) (2002). "Health care operations" under the Privacy Regulations covers a host of activities undertaken by a health care provider in the normal course of business including quality assessment and improvement activities, reviewing the competence or qualifications of health care professionals, conducting training programs in which students, trainees, or practitioners learn under supervision to practice or improve their skills, conducting or arranging for medical review, legal services, and auditing functions, and business planning, development and management. 45 C.F.R. § 164.501.

[FN73]. As will be discussed more fully infra Part II.B.3, the Privacy Regulations generally require that the Covered Entity limit the use and disclosure of PHI to the

minimum necessary to accomplish the intended use, disclosure or request. 45 C.F.R. § 164.502(b) (2002).

[FN74]. 45 C.F.R. § 164.502(a)(1)(iii) (2002). Originally, the Privacy Regulations did not address incidental uses and disclosures of PHI. As a result, many argued that the Privacy Regulations absolutely restricted the incidental use and disclosure of PHI and that this restriction would "impede many activities and communications essential to effective and timely treatment of patients." Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,193. Because the Privacy Regulations were not intended "to impede customary and necessary health care communications or practices, nor to require that all risk of incidental use or disclosure be eliminated to satisfy its standards," the Privacy Regulations were modified in August 2002 to specifically address the incidental use and disclosure of PHI. Id.

[FN75]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,194.

[FN76]. GUIDANCE, supra note 70, at 5 and HHS FAQs, supra note 65, at Must facilities have private or soundproof rooms to prevent conversations from being overheard?

[FN77]. HHS makes clear that the Privacy Regulations "explicitly permits the incidental disclosures that may result from" calling names in a waiting room or maintaining a sign-in sheet so long as the covered entity implements reasonable safeguards and the minimum necessary standard. HHS FAQs, supra note 65, at May health care providers use sign-in sheets or call out names in waiting rooms? "For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician)." Id.

[FN78]. GUIDANCE, supra note 70, at 5. HHS makes clear that the Privacy Regulations are not intended to limit communications between a health care provider and her patients so long as reasonable safeguards are put in place to limit the PHI disclosed. "For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back." HHS FAQs, supra note 65, at May health care providers leave messages at patients' homes or mail reminders to their homes?

[FN79]. 45 C.F.R. § 164.530(a)(1)(i) (2002).

[FN80]. 45 C.F.R. § 164.508(a)(1) (2002). For a more detailed discussion about the requirements for authorizations as of the date of the final modifications to the Privacy Regulations, see Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,219-23.

[FN81]. 45 C.F.R. § 164.508(b)(4) (2002).

[FN82]. 45 C.F.R. § 164.508(b)(5)(i) (2002). An authorization also cannot be revoked to the extent that the authorization was obtained as a condition of obtaining insurance coverage and "other law provides the insurer with the right to contest a claim under the policy or the policy itself." 45 C.F.R. § 164.508(b)(5)(ii) (2002).

[FN83]. 45 C.F.R. § 164.508(c)(3) (2002).

[FN84]. 45 C.F.R. § 164.508(c)(1)(i) (2002).

[FN85]. 45 C.F.R. § 164.508(c)(1)(ii) (2002).

[FN86]. 45 C.F.R. § 164.508(c)(1)(iii) (2002).

[FN87]. 45 C.F.R. § 164.508(c)(1)(iv) (2002).

[FN88]. 45 C.F.R. § 164.508(c)(1)(v) (2002). The use of authorizations in the context of research is discussed more fully infra Part II.D.3.a.

[FN89]. 45 C.F.R. § 164.508(c)(1)(vi) (2002). Where the authorization is signed by a personal representative, the authorization should describe the capacity in which the individual is signing. Id. The ability of personal representatives to act on behalf of individuals is discussed in more detail infra Part II.B.4.b.

[FN90]. A Covered Entity may either list the exceptions to the right to revoke in the authorization or, if such exceptions are set forth in a Covered Entity's Privacy Notice, provide a reference to the relevant section of the Notice. 45 C.F.R. § 164.508(c)(2)(i)(A), (B) (2002).

[FN91]. The authorization must state, as applicable, either (A) that the Covered Entity may not condition treatment and payment on whether the individual signs an authorization, or (B) in those instances in which treatment and payment may be conditioned upon obtaining a valid authorization, the consequences to the individual of refusing to sign the authorization. 45 C.F.R. § 164.508(c)(2)(ii)(A), (B) (2002).

[FN92]. 45 C.F.R. § 164.508(c)(2)(iii) (2002). See 45 C.F.R. § 164.508(c)(2) (2002) for the statements that must be set forth in an authorization.

[FN93]. It is important to consult applicable state law to ensure that the authorization also contains those elements required by state law. For instance, in New York, there are special requirements relating to the disclosure of records containing HIV information. N.Y. Pub. Health Law § 27-F (McKinney 2002); NY Comp. Codes R. & Regs. tit. 10, § 63 (2002); and NY Comp. Codes R. & Regs. tit. 14, § § 505, 633.19 (2002). Accordingly, in New York, in order to release HIV information, it is not enough that an authorization be HIPAA-compliant; the disclosure must also comply with the requirements of New York State law.

In addition, an authorization can, in most cases, be combined with other authorization forms. However, except with respect to research authorizations, an authorization generally may not be combined with any other document, such as a notice of privacy practices or consent. 45 C.F.R. § 164.508(b)(3) (2002).

Finally, because the requirements for an authorization in the context of research are slightly different, a university can draft one form of authorization for its health care providers and one for use in research studies. The effect of the Privacy Regulations on research is discussed more fully infra Part II.D.3.

[FN94]. The checklist should also reflect any particular state law requirements.

[FN95]. It is important to note that an authorization is also not valid if it is known by the Covered Entity to have been revoked or if the Covered Entity knows that any material information in the authorization is false. 45 C.F.R. § 164.508(b)(2) (2002). A university may want to include these concepts in its policies and procedures.

[FN96]. 45 C.F.R. § § 164.508(b)(6), 164.530(j) (2002).

[FN97]. 45 C.F.R. § 164.510 (2002).

[FN98]. Id.

[FN99]. 45 C.F.R. § 164.510(a)(1) (2002). In addition, a Covered Entity may disclose an individual's religious affiliation to a clergy member. Id.

[FN100]. 45 C.F.R. § 164.510(a)(2) (2002). There are, however, circumstances under which such information may be disclosed in the event of an emergency. 45 C.F.R. § 164.510(a)(3) (2002).

[FN101]. 45 C.F.R. § 164.510(b)(1), (2) (2002). The PHI disclosed should be relevant to the person's involvement with the individual's care or payment related to the individual's care. PHI may be used or disclosed in other instances by a university either with an individual's agreement or where the provider believes, in her professional judgment, that the use or disclosure is necessary. For instance, a university may use or disclose PHI "to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death." 45 C.F.R. § 164.510(b)(1)(ii) (2002). If the individual is not present or cannot agree or object due to incapacity or an emergency, then a university may use or disclose PHI if it determines, in its professional judgment, that such use or disclosure is in the best interests of the individual. 45 C.F.R. § 164.510(b)(3) (2002). Finally, a university may also use and disclose PHI under certain circumstances in connection with disaster relief efforts. 45 C.F.R. § 164.510(b)(4) (2002).

[FN102]. 45 C.F.R. § 164.510(b)(3) (2002).

[FN103]. Of course, if the physician has been expressly advised by the patient that a specified friend or family member should not receive information, the patient's wishes should be honored.

[FN104]. 45 C.F.R. § 164.530(a)(1)(i) (2002).

[FN105]. 45 C.F.R. § 164.512 (2002).

[FN106]. 45 C.F.R. § 164.512(a) (2002).

[FN107]. 45 C.F.R. § 164.512(b) (2002).

[FN108]. 45 C.F.R. § 164.512(c) (2002).

[FN109]. 45 C.F.R. § 164.512(d) (2002).

[FN110]. 45 C.F.R. § 164.512(e) (2002).

[FN111]. 45 C.F.R. § 164.512(f) (2002).

[FN112]. 45 C.F.R. § 164.512(g) (2002).

[FN113]. 45 C.F.R. § 164.512(h) (2002).

[FN114]. 45 C.F.R. § 164.512(i) (2002). Given its importance to universities, use and disclosure of PHI for research purposes will be discussed more fully infra Part II.D.3.

[FN115]. 45 C.F.R. § 164.512(j) (2002).

[FN116]. 45 C.F.R. § 164.512(k) (2002).

[FN117]. 45 C.F.R. § 164.512(l) (2002).

[FN118]. 45 C.F.R. § 164.502(b)(1) (2002).

[FN119]. HHS FAQs, supra note 65, at How are covered entities to determine what is the minimum necessary information? Although it is up to the university to reasonably determine what is the minimum information that may be used, disclosed, or requested, the Privacy Regulations make clear that the use or disclosure of, or request for, an entire medical record is not acceptable unless the entire medical record "is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request." 45 C.F.R. § 164.514(d)(5) (2002). This justification need not be undertaken on a case-by-case basis so long as "the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes." HHS FAQs, supra note 65, at Under what conditions may a health care provider use, disclose, or request an entire medical record?

[FN120]. 45 C.F.R. § 164.502(b)(2) (2002). Other circumstances under which the minimum necessary standard is not applicable include disclosures to HHS as required by the Privacy Regulations, uses or disclosures required by law, and any other uses or disclosures necessary to comply with the Privacy Regulations. Id.

[FN121]. The Privacy Regulations do, however, provide a university "with substantial discretion with respect to how it implements the minimum necessary standard, and appropriately and reasonably limits access to identifiable health information

within" the university. HHS FAQs, supra note 65, at Won't the minimum necessary restriction impede the delivery of quality health care?

[FN122]. 45 C.F.R. § 164.514(d)(2)(i) (2002).

[FN123]. 45 C.F.R. § 164.514(d)(3), (4) (2002). Because many universities provide training to medical residents, medical students, nursing students, and other medical trainees who train in covered components of the university, it is important to note that the minimum necessary standard does not prohibit those students from accessing PHI. A university, however, should make sure that its minimum necessary policies and procedures allow such medical trainees access to PHI, including entire medical records. The impact of the Privacy Regulations on student training is discussed more fully infra Part II.D.1.

[FN124]. 45 C.F.R. § 164.514(d)(3)(i), (4)(ii) (2002).

[FN125]. 45 C.F.R. § 164.514(d)(3)(ii), (4)(iii) (2002).

[FN126]. Id.

[FN127]. "Workforce" is defined under the HIPAA regulations as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." 45 C.F.R. § 160.103 (2002).

[FN128]. Id.

[FN129]. Id. It is possible for a Covered Entity to be a business associate of another Covered Entity. Id. However, a Covered Entity which is part of an OHCA does not become a business associate of other Covered Entities participating in the OHCA simply by performing a "business associate" function for the OHCA. Id.

[FN130]. 45 C.F.R. § 164.502(e)(1)(i) (2002).

[FN131]. 45 C.F.R. § 164.502(e)(1)(ii)(A) (2002). For instance, a health care provider is not required to have a business associate contract with a laboratory to whom it sends specimens nor must a hospital laboratory have a business associate contract to disclose PHI to a reference laboratory. GUIDANCE, supra note 70, at 18.

[FN132]. 45 C.F.R. § 514(e)(2) (2002).

[FN133]. For purposes of this discussion, "business associate agreement" refers to the contract or other written agreement or arrangement entered into with the business associate in order to obtain the business associate's reasonable assurances as required by the Privacy Regulations.

[FN134]. 45 C.F.R. § 164.504(e)(2) (2002). The Privacy Regulations set forth more fully what is required to be included in a business associate agreement.

[FN135]. 45 C.F.R. § 164.504(e)(1)(ii) (2002).

[FN136]. GUIDANCE, supra note 70, at 18. See also HHS FAQs, supra note 65, at Is a business associate contract needed for janitorial services and the like?

[FN137]. Id. at 19.

[FN138]. Id.

[FN139]. A university must enter into business associate agreements with all business associates with whom it enters into a relationship on a prospective basis. In addition, a university is deemed to be in compliance with the Privacy Regulations if it entered into a written agreement with its business associate prior to October 15, 2002, and the agreement was not renewed or modified from October 15, 2002, to April 14, 2003. Such an agreement will be deemed compliant until the earlier of the date upon which the agreement is renewed or modified or April 14, 2004. 45 C.F.R. § 164.533(d) (2002).

The process for securing business associate agreements with business associates will be affected by the manner in which a university enters into contracts generally. For instance, where agreements routinely receive legal review, the university's lawyers must be familiar with the business associate requirements and ensure that business associate agreements are secured. In other cases, some forms of agreement, including those with business associates, may go through a purchasing department. In those cases, the purchasing department staff must be familiar with the business associate provisions of the Privacy Regulations to ensure compliance. For those purchasing operations that employ standard terms and conditions, it may be a challenge to try to incorporate the business associate terms into the terms and conditions in such a way that will satisfy the Privacy Regulations.

[FN140]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,264, available at http:// www.hhs.gov/ocr/hipaa/contractprov.html (last visited Apr. 14, 2003).

[FN141]. Whichever form is used, it is recommended that the agreement contain an indemnity, if possible, from the business associate to the university for potential violations of the business associate agreement or the Privacy Regulations. While an indemnity is not required by the Privacy Regulations, it provides a university with added protection against HIPAA violations by business associates.

[FN142]. 45 C.F.R. § 164.502(g) (2002).

[FN143]. GUIDANCE, supra note 70, at 11.

[FN144]. 45 C.F.R. § 164.502(g) (2002).

[FN145]. 45 C.F.R. § 164.502(g)(2) (2002).

[FN146]. 45 C.F.R. § 164.502(g)(3) (2002).

[FN147]. 45 C.F.R. § 164.502(g)(4) (2002).

[FN148]. 45 C.F.R. § 164.502(g)(5) (2002).

[FN149]. 45 C.F.R. § 164.530(a)(1)(i) (2002).

[FN150]. Job descriptions for the role of privacy officer are available on the web and may be helpful to those universities attempting to understand the responsibilities that their privacy officers will assume. See, e.g., http://www.ahima.org/infocenter/models/PrivacyOfficer2001.cfm (last visited Apr. 12, 2003). Other resources are available at http://www.massmed.org/search/results.asp?userneed@TheForefront-HIPAA (last visited Apr. 12, 2003).

[FN151]. 45 C.F.R. § 164.530(a)(1)(ii) (2002).

[FN152]. 45 C.F.R. § 164.520(a)(1) (2002).

[FN153]. 45 C.F.R. § 164.520(b)(1) (2002). In addition, health care providers may have an obligation to translate the Notice into different languages pursuant to Title VI of the Civil Rights Act of 1964 and its implementing regulation. 42 U.S.C. § 2000d (2000); 45 C.F.R. § 80 (2002). It has been HHS' position "that in order to avoid discrimination against [Limited English Proficiency] persons on the grounds of national origin, health and social service providers must take adequate steps to ensure that such persons receive the language assistance necessary to afford them meaningful access to their services, free of charge." Policy Guidance on the Prohibition Against National Origin Discrimination as it Affects Persons with Limited English Proficiency, 65 Fed. Reg. 52762 (Aug. 30, 2000) ("Policy Guidance"). A more detailed discussion of the extent to which health care providers must translate written documents into languages other than English is contained in the Policy Guidance. Id. See also Federally Mandated Language Access for Limited English Proficient Persons, prepared by the Health Consumer Alliance, available at www.healthconsumer.org (last visited Apr. 23, 2003).

[FN154]. 45 C.F.R. § 164.520(b)(1)(ii) (2002). The Notice of Privacy Practices must also reflect any limitations on uses and disclosures, otherwise permitted by the Privacy Regulations, that are imposed by state law and survive HIPAA preemption. 45 C.F.R. § 164.520(b)(2) (2002).

[FN155]. 45 C.F.R. § 164.520(b)(1)(iii)(A) (2002).

[FN156]. 45 C.F.R. § 164.520(b)(1)(iv) (2002).

[FN157]. 45 C.F.R. § 164.520(b)(1)(v) (2002).

[FN158]. 45 C.F.R. § 164.520(b)(1)(vi) (2002).

[FN159]. 45 C.F.R. § 164.520(b)(1)(vii) (2002). The Notice must also prominently display the following header: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE

REVIEW IT CAREFULLY." 45 C.F.R. § 164.520(b)(1)(i) (2002).

[FN160]. HHS FAQs, supra note 65, at Are covered entities permitted to give individuals a "layered" notice? Even where a summary is provided, the full Notice of Privacy Practices must be provided.

[FN161]. 45 C.F.R. § 164.520(c)(2)(i) (2002). Universities should also consider whether there may be circumstances under which their health care providers' first treatment encounter is other than face-to-face. In those cases, while a Notice of Privacy Practices must still be provided to an individual, the university can use its reasonable discretion about how best to fulfill its obligations:

For example, a health care provider who first treats a patient over the phone satisfies the notice provision requirements of the Privacy Rule by mailing the notice to the individual the same day, if possible. To satisfy the requirement that the provider also make a good faith effort to obtain the individual's acknowledgement of the notice, the provider may include a tear- off sheet or other document with the notice that requests that the acknowledgement be mailed back to the provider. The health care provider is not in violation of the Rule if the individual chooses not to mail back an acknowledgement; and a file copy of the form sent to the patient would be adequate documentation of the provider's good faith effort to obtain the acknowledgement.

HHS FAQs, supra note 65, at How do I provide notice and get an acknowledgement when the first encounter is not face-to-face?

[FN162]. 45 C.F.R. § 164.520(c)(2)(i)(B) (2002).

[FN163]. 45 C.F.R. § 164.520(c)(2)(ii) (2002). It should be noted that state law requirements for obtaining consent from an individual for treatment or for use of the individual's medical information are separate from, and not a substitute for, the Privacy Regulation's requirement that Covered Entities obtain an individual's acknowledgement that the Covered Entity's Notice of Privacy Practices has been provided. HHS FAQs, supra note 65, at How does the HIPAA Privacy Rule change the laws concerning the consent for treatment?

[FN164]. 45 C.F.R. § § 164.520(e), 164.530(j) (2002).

[FN165]. 45 C.F.R. § 164.520(c)(2)(i)-(ii) (2002).

[FN166]. 45 C.F.R. § 164.520(b)(3) (2002).

[FN167]. 45 C.F.R. § 164.520(c)(2)(ii) (2002).

[FN168]. GUIDANCE, supra note 70, at 42.

[FN169]. 45 C.F.R. § 164.524(a)(1) (2002). The Privacy Regulations address the form in which access to PHI must be provided to individuals, the time and manner in which access must be provided, and the fees that Covered Entities may charge individuals for access to PHI. 45 C.F.R. § 164.524(c)(2)-(4) (2002). Subject to the requirements of state law, it is also important to note that the Privacy Regulations set forth circumstances under which individuals do not have a right to inspect and copy their PHI. For instance, individuals do not have a right under the Privacy Regulations to inspect and copy psychotherapy notes or information compiled in

anticipation of litigation. See 45 C.F.R. § 164.524(a)(1)(i)-(iii) (2002).

[FN170]. A designated record set includes, inter alia, medical and billing records "maintained by or for" the Covered Entity. 45 C.F.R. § 164.501 (2002). The Covered Entity must document the designated record sets that are "subject to access by individuals ...." 45 C.F.R. § 164.524(e)(1) (2002).

[FN171]. 45 C.F.R. § 164.524(b)(1) (2002).

[FN172]. 45 C.F.R. § 164.524(b)(2) (2002). Again, state law should be consulted to determine whether shorter response times may be required.

[FN173]. 45 C.F.R. § 164.524(b)(2)(iii) (2002).

[FN174]. In fact, the Privacy Regulations require that Covered Entities document the titles of the persons or offices responsible for receiving and processing requests for PHI. 45 C.F.R. § 164.524(e)(2) (2002).

[FN175]. 45 C.F.R. § 164.524(a)(2) (2002). In addition, it is important to examine state law to determine whether it requires access to PHI that the Privacy Regulations otherwise permit a provider to deny. In such cases, because state law is more favorable to patients, access would have to be granted.

[FN176]. 45 C.F.R. § 164.524(a)(3) (2002).

[FN177]. 45 C.F.R. § 164.524(d)(4) (2002). The Privacy Regulations should be consulted for a more detailed discussion of what the review process requires.

[FN178]. 45 C.F.R. § 164.528(a)(1) (2002).

[FN179]. Initially, the accounting requirements also would have applied to uses or disclosures made pursuant to an individual's authorization. However, in response to public comments, HHS decided to eliminate the requirement because the "authorization process itself adequately protects individual privacy by assuring that the individual's permission is given both knowingly and voluntarily." Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,244.

[FN180]. 45 C.F.R. § 164.528(a)(1) (2002). Other disclosures which are not subject to the accounting obligation include disclosures (a) for facility directory or to persons involved in patient's care, (b) for national security or intelligence purposes, (c) to correctional institutions or law enforcement officials, (d) as part of a limited data set, and (e) that occurred prior to the compliance date. Id.

[FN181]. A "limited data set" is PHI that excludes certain direct identifiers enumerated in the Privacy Regulations, including name, telephone number, and medical record numbers, which may be disclosed for research, public health, or health care operations if a data use agreement is entered into with the party receiving the data set. 45 C.F.R. § 164.514(e)(2), (3) (2002). Use of limited data sets for research is discussed more fully infra Part II.D.3.c.

[FN182]. A law enforcement agency or health oversight agency may temporarily suspend an individual's right to receive an accounting of the disclosures to the law enforcement agency or health care oversight agency in certain instances. See 45 C.F.R. § 164.528(a)(2) (2002).

[FN183]. 45 C.F.R. § 164.528(b) (2002). A university must keep a copy of the accounting for six years. 45 C.F.R. § § 164.528(d), 164.530(j) (2002).

[FN184]. 45 C.F.R. § 164.528(b)(2) (2002). If multiple disclosures have been made to the same person or entity for a single purpose (for instance, research), the accounting may provide the information noted above for the first disclosure, the frequency, periodicity, or number of disclosures made during the accounting period, and the date of the last disclosure. 45 C.F.R. § 164.528(b)(3) (2002).

[FN185]. 45 C.F.R. § 164.528(b)(4)(i) (2002). HHS refused to adopt commenters' proposals to eliminate the accounting requirement completely with respect to research disclosures. However, HHS did recognize that to require a detailed accounting as originally contemplated "could have the undesired effect of causing covered entities to halt disclosures of protected health information for research." Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,245. Accordingly, HHS revised the accounting requirements for research as set forth above.

[FN186]. 45 C.F.R. § 164.528(b)(4)(i)(A)-(F) (2002).

[FN187]. 45 C.F.R. § 164.528(c)(1) (2002).

[FN188]. See 45 C.F.R. § 164.528(c)(2) (2002).

[FN189]. 45 C.F.R. § § 164.522, 164.526 (2002).

[FN190]. 45 C.F.R. § 164.526(a) (2002). Importantly, health information need not be amended if a university determines that the information is "accurate and complete." 45 C.F.R. § 164.526(a)(2)(iii) (2002).

[FN191]. 45 C.F.R. § 164.522(a) (2002). A university is not required to agree to a requested restriction. 45 C.F.R. § 164.522(a)(1)(ii) (2002).

[FN192]. For purposes of this discussion, it is assumed that the facilities to which students are being sent to receive clinical training are covered by the Privacy Regulations.

[FN193]. 45 C.F.R. § 160.103 (2002).

[FN194]. That students are part of the training facility's workforce is also consistent with the definition of "health care operations" under the Privacy Regulations. Under the Privacy Regulations, "health care operations" includes "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health

care providers ...." 45 C.F.R. § 164.501 (2002).

[FN195]. See supra Part II.A, which discusses how to determine whether a university is a Covered Entity.

[FN196]. See 20 U.S.C. § 1232g(a)(4)(B)(iv) (2000). For a more detailed discussion of the interaction between FERPA and HIPAA, see supra Part II.B.1.a.

[FN197]. See id. For a more detailed discussion of the interaction between FERPA and HIPAA, see supra Part II.B.1.a.

[FN198]. HHS, of course, does not believe that the Privacy Regulations will hinder medical research. HHS FAQs, supra note 65, at Will the Privacy Rule make covered entities unable or reluctant to share information for research? ("Indeed, patients and health plans members should be more willing to authorize disclosures of their information for research and to participate in research when they know their information is protected.").

[FN199]. Universities that have both researchers who need access to PHI and covered components that provide health care will have to address the requirements of the Privacy Regulations from two perspectives: that of the researcher trying to obtain access to PHI for research purposes from a Covered Entity (which may be itself or a third-party) and that of a Covered Entity from whom PHI is being requested. Indeed, those universities, which also may have an Institutional Review Board ("IRB") or Privacy Board, will face a formidable training task; researchers will need to be educated about what the Privacy Regulations require before they will be permitted access to PHI, health care providers must be trained about the requirements for using or disclosing PHI for research purposes, and the members of the IRB or Privacy Board will need to be trained about their new responsibilities under the Privacy Regulations.

[FN200]. A university or other Covered Entity may use or disclose for research PHI received before or after April 14, 2003, if it obtained, prior to April 14th, either an authorization or express permission to use or disclose PHI for research, an informed consent to participate in research, or a waiver of informed consent from an IRB (provided that if informed consent is sought from an individual after April 14th, an authorization must be obtained). 45 C.F.R. § 164.532(c) (2002).

[FN201]. See supra Part II.B.2.c for a discussion of the use and disclosure of PHI by a Covered Entity pursuant to an authorization.

[FN202]. 45 C.F.R. § 164.508(b)(4)(i) (2002). The Privacy Regulations set forth two other circumstances under which enrollment and treatment may be conditioned upon the provision of an authorization that relate to health plans and health care provided for the purpose of creating PHI. See 45 C.F.R. § 164.508(b)(4)(ii), (iii) (2002).

[FN203]. 45 C.F.R. § 164.508(b)(3)(i) (2002). The Privacy Regulations set forth two other circumstances under which an authorization may be combined with another document. See 45 C.F.R. § 164.508(b)(3)(ii), (iii) (2002).

[FN204]. 45 C.F.R. § 164.508(c)(v) (2002). The requirement that a research authorization contain an expiration date or event was removed in August 2002 as a

result of comments received by HHS detailing the legitimate uses and disclosure that researchers need to continuously make, sometimes after a research study has ended. See Mark Barnes & Clinton Hermes, Clinical Research After the August 2002 Privacy Rule Amendments, 1 BUREAU OF NAT'L AFF. MED. RES. L. & POL. REP. 406, 408 (2002) (containing an excellent discussion of the application of the final Privacy Regulations to research).

[FN205]. See 45 C.F.R. § 164.508(b)(5) (2002).

[FN206]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,224. See also Barnes & Hermes, supra note 204, at 406.

[FN207]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,225. HHS gave examples of the effect of its clarification, stating that continued use and disclosure of PHI based on the "reliance exception" would be permitted "to account for a subject's withdrawal from the research study, as necessary to incorporate the information as part of a marketing application submitted to the FDA, to conduct investigations of scientific misconduct, or to report adverse events." Id. However, a Covered Entity may not rely on the exception "to continue disclosing additional protected health information to a researcher or to use for its own research purposes information not already gathered at the time an individual withdraws his or her authorization." Id.

[FN208]. 45 C.F.R. § 164.512(i)(1) (2002). It is important to remember that many uses and disclosures of PHI for research purposes are subject to the accounting requirements of the Privacy Regulations. For a more detailed discussion of the accounting requirements generally and as they relate to uses and disclosures of PHI for research, see supra Part II.C.4.

[FN209]. See 45 C.F.R. § 164.512(i)(1)(ii)-(iii) (2002) for the specific requirements of the Privacy Regulations relating to the use and disclosure of PHI for research purposes for reviews preparatory to research and with respect to the review of decedent's information.

[FN210]. See 45 C.F.R. § 164.512(i)(1)(i)(B) (2002) for the requirements of the composition of a Privacy Board. It is important to note that it is not necessary that the Covered Entity using or disclosing PHI for research have its own IRB or Privacy Board. "The IRB or Privacy Board could be created by the covered entity or the recipient researcher, or it could be an independent board." HHS FAQs, supra note 65, at Must I create an IRB or Privacy Board before using or disclosing information for research?

[FN211]. 45 C.F.R. § 164.512(i)(2)(ii) (2002). One of the instances in which a waiver may be sought is for the use or disclosure of PHI to create a research database. HHS FAQs, supra note 65, at Is the creation of a database for research permissible with an IRB/Privacy Board waiver? Thereafter, use of the PHI maintained in the database for research could be made with the individual's authorization or under those circumstances permitted by the Privacy Regulations without an authorization. Id.

[FN212]. 45 C.F.R. § 164.512(i)(2)(ii)(A) (2002).

[FN213]. 45 C.F.R. § 164.512(i)(2)(ii) (2002).

[FN214]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,229.

[FN215]. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,230.

[FN216]. See supra Part II.B.1.b, which describes the process for de- identifying PHI.

[FN217]. 45 C.F.R. § 164.514(e) (2002). The concept of permitting access to a limited data set for research purposes was added to the Privacy Regulations in August 2002. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,234-38. The research community had expressed concerns that "the de-identification standard in the Privacy Rule could curtail important research, public health, and health care operations activities." Id. at 53,234. In particular, "researchers raised concerns that the impracticality of using de-identified data would significantly increase the workload of IRBs because waivers of individual authorization would need to be sought more frequently for research studies even though no direct identifiers were needed for the studies." Id. Accordingly, the concept of a limited data set was created so that access for research purposes could be granted to data that contained more information than would qualify under the de-identification standard.

[FN218]. 45 C.F.R. § 164.514(e)(2) (2002).

[FN219]. 45 C.F.R. § 164.514(e)(4) (2002). Researchers within a university may be asked by other health care providers to enter into data use agreements where the researchers are attempting to gain access to limited data sets of Covered Entities.

[FN220]. 45 C.F.R. § 164.514(e)(4)(ii) (2002).

[FN221]. Although not defined in the Privacy Regulations, the preamble to the Regulations issued in December 2000 defined demographic information in the context of fundraising as including "name, address and other contact information, age, gender, and insurance status." Standards for the Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,718 (Dec. 28, 2000) (codified at 45 C.F.R. § § 160, 164 (2002)).

[FN222]. 45 C.F.R. § 164.514(f)(1) (2002).

[FN223]. See 45 C.F.R. § 164.508 (2002).

[FN224]. This applies to fundraising literature requiring an authorization, such as literature based on, or related to, an individual's diagnosis. As long as the practice is included in a university's Notice of Privacy Practices, a university can also send to individuals general fundraising literature as permitted by § 164.514(f) of the Privacy Regulations.

[FN225]. 45 C.F.R. § 164.508(b)(5) (2002) ("An individual may revoke an

authorization ... at any time ....").

[FN226]. A university may also consider alternative methods for ascertaining the interests of potential donees. In that way, a university could direct fundraising materials to an individual based on the individual's expressed interest.

[FN227]. 45 C.F.R. § 164.514(f)(2)(i) (2002).

[FN228]. 45 C.F.R. § 164.514(f)(2)(ii), (iii) (2002).

[FN229]. 45 C.F.R. § 164.501 (2002).

[FN230]. GUIDANCE, supra note 70, at 26.

[FN231]. 45 C.F.R. § 164.501 (2002). Disease management, health promotion, preventative care, and wellness programs also do not fall under the Privacy Regulations' definition of marketing. GUIDANCE, supra note 70, at 26- 27.

[FN232]. GUIDANCE, supra note 70, at 27.

[FN233]. 45 C.F.R. § 164.508(a)(3)(i) (2002).

[FN234]. GUIDANCE, supra note 70, at 28.

[FN235]. 45 C.F.R. § 160.102 (2002).

[FN236]. See 45 C.F.R. § 160.103 (2002) for a complete definition of "health plan" under the Privacy Regulations. Section 160.103 also sets forth the definition of "group health plans" and includes plans that provide benefits to fifty or more participants or is administered by an entity other than the employer that established and maintains the plan. See also Dan Roble & Patrik S. Florencio, HIPAA in Employment and Educational Facilities, 8 BUREAU OF NAT'L AFF. HEALTH PLAN & PROVIDER REP. 1200, 1201 (2002).

[FN237]. Id.

[FN238]. 45 C.F.R. § 160.103 (2002). See also Roble & Florencio, supra note 236, at 1204.

[FN239]. 45 C.F.R. § 160.103; 42 U.S.C. 300gg-91(c)(1)(A),(B), and (C) (2000). See also Roble & Florencio, supra note 236, at 1204.

[FN240]. 45 C.F.R. § 160.103. See also Roble & Florencio, supra note 236, at 1204.

[FN241]. Roble & Florencio, supra note 236, at 1204.

[FN242]. Id.

[FN243]. Id.

[FN244]. "Self-funded group health plans dispense health benefits to enrollees through a third party (i.e., the group health plan pays for enrollee claims through a [third-party administrator]); rather than via a health insurance issuer/HMO." Roble & Florencio, supra note 236, at 1204.

[FN245]. The administrative requirements of the different types of health plans will be discussed more fully at infra Part III.C.

[FN246]. Roble & Florencio, supra note 236, at 1204-05.

[FN247]. Similarly, a university should determine whether any of its plans are hybrid entities, and consider making the necessary hybrid declaration. See discussion of hybrid entities supra Part II.A.1. For instance, to the extent the university uses its form 550 to define its plan, the 550 may contain both plans covered by the Privacy Regulations and plans that are not. In order to avoid subjecting the non-HIPAA covered products to the rigors of the Privacy Regulations, the plan should be designated a hybrid entity.

[FN248]. 45 C.F.R. § 164.501 (2002).

[FN249]. 45 C.F.R. § 164.514(a), (b) (2002). De-identified Information is discussed more fully supra Part II.B.1.b.

[FN250]. 45 C.F.R. § 164.504(f)(1)(ii) (2002).

[FN251]. 45 C.F.R. § 164.504(f)(1)(iii) (2002).

[FN252]. 45 C.F.R. § § 164.504(f)(2), (f)(3)(i) (2002). The obligations that a plan sponsor who receives PHI are obligated to undertake as reflected in the required amendment to the plan's plan documents are not unlike the obligations assumed by a business associate through a business associate agreement.

[FN253]. 45 C.F.R. § 164.504(f)(2)(ii) (2002).

[FN254]. A university can also take this opportunity to determine whether it needs to continue to receive all of the information it currently gets. To the extent that a university receives PHI that it does not necessarily need, the better practice would be to stop receiving such information.

[FN255]. For a discussion of the administrative requirements imposed on covered health care providers under the Privacy Regulations, see supra Part II.C.

[FN256]. 45 C.F.R. § § 160.103, 164.502 (2002). For a more detailed discussion of business associates under the Privacy Regulations, see supra Part II.C.2.

[FN257]. 45 C.F.R. § 164.520 (2002).

[FN258]. 45 C.F.R. § 164.520(b)(1) (2002). For a more detailed discussion of the requirements concerning the Notice of Privacy Practices, see supra Part II.C.3.

[FN259]. 45 C.F.R. § 164.530(a)(1)(i) (2002).

[FN260]. For a more detailed discussion of the requirements of the Privacy Regulations with respect to privacy officials, see supra Part II.C.1.

[FN261]. 45 C.F.R. § 164.524 (2002). For a more detailed discussion of the access requirements under the Privacy Regulations, see supra Part II.C.3. It may be that arrangements can be made with the health plan's third-party administrator to administer the processes relating to the exercise of a plan member's individual rights. This may make particular sense where the third party administrator maintains the plan's designated record set and otherwise performs similar administrative functions on behalf of the plan.

[FN262]. 45 C.F.R. § 164.528 (2002). For a more detailed discussion of the accounting requirements under the Privacy Regulations, see supra Part II.C.4.

[FN263]. 45 C.F.R. § 164.522 (2002). For a more detailed discussion of the requirements relating to requests for amendment to PHI under the Privacy Regulations, see supra Part II.C.5.

[FN264]. 45 C.F.R. § 164.526 (2002). For a more detailed discussion of the requirements relating to requests for additional privacy protections under the Privacy Regulations, see supra Part II.C.5.

[FN265]. 45 C.F.R. § 164.502(b)(1) (2002). The minimum necessary requirements under the Privacy Regulations are discussed supra Part II.B.3.

[FN266]. Health Plan Sponsorship is at Heart of Employer Responsibilities, REP. ON MEDICARE COMPLIANCE (Oct. 3, 2002), available at http:// www.aishealth.com/Compliance/Hipaa/RMChealtPlan.html (last visited Apr. 11, 2003).

[FN267]. Roble & Florencio, supra note 236, at 1204. See 45 C.F.R. § § 164.520(a)(2)(iii), 164.530(k) (2002). For a discussion of the Privacy Regulations' requirements with respect to the amendment of plan documents, see supra Part III.B.

[FN268]. Roble & Florencio, supra note 236, at 1204. See 45 C.F.R. § 164.520(a)(2)(ii) (2002).

[FN269]. 45 C.F.R. § 164.530(b) (2002).

[FN270]. 45 C.F.R. § 164.530(b)(2)(i)(C) (2002).

[FN271]. 45 C.F.R. § 164.530(b)(2)(ii) (2002).

[FN272]. As previously discussed, a research university will have additional training obligations for its research staff and members of its IRB or Privacy Board. See supra Part II.D.3.

[FN273]. HHS FAQs, supra note 65, at Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?

[FN274]. Id.

[FN275]. 45 C.F.R. § 164.530(a)(1)(ii) (2002). See supra Part II.c.1.

[FN276]. 45 C.F.R. § 164.530(d)(1) (2002). Universities are also required to document any complaints, including the disposition of complaints. 45 C.F.R. § 164.530(d)(2) (2002).

[FN277]. 45 C.F.R. § 164.530(e)(1) (2002).

[FN278]. 45 C.F.R. § 164.530(e)(2) (2002).

[FN279]. 45 C.F.R. § 160.306(a) (2002). The Privacy Regulations also set forth particular requirements with respect to the filing of complaints with HHS. See 45 C.F.R. § 160.306(b) (2002). Information on how to file a complaint, including the information to be included in a complaint and where complaints should be sent, can be found at http.// www.hhs.gov/ocr/howtofileprivacy.htm.

[FN280]. Office for Civil Rights, Statement of Delegation of Authority, 65 Fed. Reg. 82, 381 (Dec. 28, 2000).

[FN281]. 45 C.F.R. § 160.306(c) (2002).

[FN282]. 45 C.F.R. § 160.308 (2002).

[FN283]. 42 U.S.C. § § 1320d(5)-(6) (2000). HHS has published interim "rules of procedure to inform regulated entities of our approach to enforcement and to advise enforcing the Privacy Regulations. See http:// www.hhs.gov/ocr/moneypenalties.html (last visited Apr. 23, 2003).

[FN284]. 42 U.S.C. § 1320d(5)(a)(1) (2000). No penalty will be imposed by HHS, however, if HHS determines that the university "did not know, and by exercising reasonable diligence would not have known," of the violation. 42 U.S.C. § 1320d(5)(b)(2) (2000). In addition, HHS may not impose a penalty if the failure to comply was "due to reasonable cause and not to willful neglect," or if the failure "is corrected during the 30-day period beginning on the first date" the university "knew, or by exercising reasonable diligence would have known, that the failure to

comply occurred." 42 U.S.C. § 1320d(5)(b)(3)(A) (2000).

[FN285]. 42 U.S.C. § 1320d(6) (2000).

[FN286]. 42 U.S.C. § 1320d(6)(b)(3) (2000).

END OF DOCUMENT