Vinson&Elkins V&E
ATTORNEYS AT LAW

VINSON & ELKINS L.L.P.
2300 FIRST CITY TOWER
1001 FANNIN STREET
HOUSTON, TEXAS 77002-6760
TELEPHONE (713) 758-2222
FAX (713) 758-2346
www.velaw.com

Brenda T. Strama
Direct Dial 713 758-4590
Direct Fax 713 615-5715
bstrama@velaw.com

July 2002

Application of the Privacy Standards to Integrated Delivery Systems and Other Complex Health Care Arrangements

Brenda T. Strama
Stacey A. Tovino

I. Introduction

This analysis discusses the concepts of the organized health care arrangement, the single affiliated covered entity, and the hybrid entity under the final HIPAA privacy regulations issued by the federal Department of Health and Human Services ("HHS") on December 28, 2000, (the "Privacy Standards"),[1] as amended by the proposed modifications issued by HHS on March 27, 2002 (the "Proposed Modifications").[2]

Specifically, this analysis discusses how the Privacy Standards, as amended by the Proposed Modifications, permit two or more covered entities to *aggregate* themselves either into an organized health care arrangement ("OHCA") or a single affiliated covered entity ("SACE"), and permit certain covered entities ("hybrid entities") to *segregate* themselves into their health care components ("health components") and non-health care components ("non-health components"). This Legal Analysis further discusses how the Privacy Standards, as amended by the Proposed Modifications, apply to OHCAs, SACEs, and hybrid entities.

II. Objectives

Explanation of an OHCA:

- **An OHCA Is Defined As One of Five Types of Arrangements.** An OHCA is defined as one of the following five types of arrangements: (1) a clinically integrated care setting in which individuals typically receive care from more than one health care provider; (2) an organized system of health care in which more than one covered entity participates and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and participate in at least one of three specific types of activities; (3) a group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by the health insurance issuer or HMO that relates to individuals who are or who have

been participants or beneficiaries in such group health plan; (4) a group health plan and one or more other group health plans, each of which are maintained by the same plan sponsor; or (5) the group health plans described in (4) and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relate to individuals who are or who have been participants or beneficiaries in any such group health plans.

- **Only One "Joint Notice" Needs To Be Developed for the Entire OHCA.** Covered entities that participate in an OHCA can comply with the notice of privacy practices ("Notice") requirement by developing a joint notice ("Joint Notice") that describes the entities' combined privacy practices, if certain requirements are met.

- **Uses and Disclosures for the TPO of the OHCA Are Permitted Without Consent or Authorization.** Covered entities that participate in an OHCA and that have developed a Joint Notice may disclose protected health information ("PHI") about an individual to another covered entity that participates in the OHCA for any treatment, payment, or health care operations ("TPO") activity of the OHCA without a specific consent or authorization from the individual who is the subject of the PHI.

- **Only One Privacy Official and One Contact Person Need Be Designated for the Entire OHCA**. The OHCA may designate just one privacy official and one contact person for the information collected under the Joint Notice. There is nothing in the HIPAA Privacy Standards that prohibits the privacy official and the contact person from being the same person.

Explanation of a SACE:

- **Entities Under Common Ownership or Control May Designate Themselves as a SACE.** Legally separate covered entities that are affiliated may designate themselves as a SACE if all of the covered entities are under common ownership or control.

- **Only One Notice Needs To Be Developed for the Entire SACE**. SACEs may develop, post, and distribute to each individual that receives services from the SACE, as required, a single Notice. Covered entities under common ownership or control that elect not to designate themselves as a SACE but meet the definition of an OHCA may elect to produce a Joint Notice.

- **Uses and Disclosures for the TPO of the SACE Are Permitted Without Consent or Authorization**. Covered entities that participate in a SACE and that have developed a single Notice may disclose PHI about an individual to another covered entity that participates in the SACE for any TPO activity of the recipient

covered entity without a specific consent or authorization from the individual who is the subject of the PHI.

- **Only One Privacy Official and One Contact Person Need Be Designated for the Entire SACE.** The entire SACE may designate just one privacy official and one contact person. There is nothing in the HIPAA Privacy Standards that prohibits the privacy official and the contact person from being the same person.

Explanation of hybrid entities:

- **The Privacy Standards Technically Only Apply to the Health Component(s) of the Hybrid Entity**. If your organization qualifies and chooses to identify itself as a hybrid entity, then any reference in the Privacy Standards to a "covered entity" should be read as a reference to the "health component" of the hybrid entity.

- **The Hybrid Entity Is Responsible for Ensuring Compliance with the Privacy Standards.** Although the Privacy Standards technically only apply to the health component(s) of the hybrid entity, the hybrid entity itself is responsible for ensuring that its health components do not impermissibly use or disclose protected health information, and that its non-health components do not impermissibly access protected health information. In addition, the hybrid entity is responsible for establishing safeguards to prevent the non-health components of the hybrid entity from impermissibly accessing protected health information.

III. Organized Health Care Arrangements

A. Why Are There Special Rules for OHCAs?

The Privacy Standards use the term OHCA to describe certain arrangements in which participants need to share PHI about individuals to manage and benefit the common enterprise.[3] The Privacy Standards include five arrangements within the definition of an OHCA. The arrangements range in legal structure, but a key component of each arrangement is that individuals who obtain services have an expectation that the arrangement is integrated and jointly manages its operations.

Perhaps the most common example of an OHCA is the hospital setting, in which a hospital and a physician with staff privileges at the hospital together provide treatment to the individual. The hospital and each of the physicians likely are separate covered entities to the extent each transmits health information in electronic form in connection with certain standard transactions.[4] However, the Privacy Standards recognize that the hospital and the physician participants in such a clinically integrated setting need to be able to share PHI freely not only for treatment purposes, but also to improve their joint operations. The preamble to the Privacy Standards explains that any physician with staff privileges at the hospital must be able to participate in the hospital's morbidity and mortality reviews, even when that particular physician's patients are not being discussed. Nurses and other hospital personnel also must be

able to participate in such reviews. These health care operations benefit the common enterprise, even when the benefits to a particular participant are not evident.

Without the special treatment given to OHCAs by the Privacy Standards, each separate covered entity that is part of the OHCA would have to obtain the patient's authorization before disclosing PHI to another covered entity member of the OHCA if the disclosure is not otherwise permitted without patient authorization under the amended Privacy Standards.

As background, the Proposed Modifications permit covered entities to disclose PHI for the treatment activities of another provider without consent or authorization.[5] Accordingly, one covered entity member of the OHCA certainly could disclose PHI without consent or authorization to another provider member of the OHCA for that provider's treatment activities without the special treatment given to OHCAs. Further, the Proposed Modifications permit covered entities to disclose PHI for the payment activities of another covered entity or provider without consent or authorization.[6] Accordingly, one covered entity member of the OHCA certainly could disclose PHI without consent or authorization to another member of the OHCA for that member's payment activities without the special treatment given to OHCAs. Finally, the Proposed Modifications permit covered entities to disclose PHI for certain health care operations activities of another covered entity (i.e., those activities identified in the first and second paragraphs of the definition of health care operations [e.g., quality assessment, development of clinical guidelines, peer review, training programs, etc.] as well as activities the purpose of which is health care fraud and abuse detection or compliance) without consent or authorization if both covered entities currently have or have had in the past a relationship with the individual.[7] However, a careful reading of the previous sentence illustrates that covered entities generally may not disclose PHI to another covered entity for those health care operations activities that are not included in the first and second paragraphs of the definition of health care operations or that do not relate to health care fraud and abuse detection or compliance without the individual's authorization unless the special treatment given to OHCAs is taken into account. Similarly, covered entities generally may not disclose PHI to another covered entity that does not currently have or did not have in the past a relationship with the individual without the individual's authorization unless the special treatment given to OHCAs is taken into account.

Accordingly, the special treatment given by the amended Privacy Standards to OHCAs allows covered entities that participate in an OHCA to disclose PHI about an individual to another covered entity that participates in the OHCA for ***any*** health care operation activity of the OHCA (not just those listed in the first and second paragraphs of the definition of health care operations or those relating to health care fraud and abuse detection or compliance) even when both covered entities do not have or did not have in the past a relationship with the individual.

B. How Do You Know If Your Arrangement Constitutes an OHCA?

The Privacy Standards define an OHCA as one of the following five arrangements (the last three of which relate to group health plans):

- **Clinically Integrated Health Care Setting.** A clinically integrated care setting in which individuals typically receive health care from more than one health care provider. *A common example of this type of OHCA is the hospital setting, in which a hospital and a physician with staff privileges at the hospital together provide treatment to the individual*.[8]

- **Organized System of Health Care.** An organized system of health care in which more than one covered entity participates, and in which the participating covered entities: (i) hold themselves out to the public as participating in a joint arrangement; and (ii) participate in joint activities that include at least one of the following: (a) 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); or (b) 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); or (c) 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). *A common example of this type of OHCA is an independent practice association (or "IPA") formed by a large number of physicians. They may advertise themselves as a common enterprise (e.g., Acme IPA), whether or not they are under common ownership or control, whether or not they practice together in an integrated clinical setting, and whether or not they share financial risk. If such a group engages jointly in one or more of the listed activities, the participating covered entities will need to share PHI to undertake such activities and to improve their joint operations*.[9]

- **Group Health Plan Plus Issuer or HMO.** A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to PHI *created* or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan. *Here, the Privacy Standards are recognizing that many group health plans are funded partially or fully through insurance, and that in some cases the group health plan and issuer or HMO need to coordinate operations to properly serve the enrollees*.[10]

- **Group Health Plans Maintained by the Same Plan Sponsor.** A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor. *Here, the Privacy Standards are recognizing that in some instances plan sponsors provide health benefits*

> *through a combination of group health plans, and that they may need to coordinate the operations of such plans to better serve the participants and beneficiaries of the plans*.[11]

- **Group Health Plans Maintained by the Same Plan Sponsor Plus Issuers or HMOs**. The group *health* plans described in the previous bullet and health insurance issuers or HMOs with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any such group health plans.[12] *Here, the Privacy Standards are recognizing that in some instances a plan sponsor may provide benefits through more than one group health plan, and that such plans may fund the benefits through one or more issuers or HMOs. Again, coordinating health care operations among these entities may be necessary to serve the participants and beneficiaries in the group health plans*.[13]

If your organization participates in one of these five arrangements, the Privacy Standards apply specially to your organization, as described below.[14]

C. What Is So Special About Being Part of an OHCA?

One of the special aspects about being part of an OHCA is that the individual covered entity members of an OHCA jointly may use PHI maintained by any individual member for ***any health care operation activity*** of the common enterprise.[15] The Proposed Modifications specifically amend the Privacy Standards to state that:

> A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.[16]

Importantly, the Privacy Standards define health care operations to include any of the following activities of the covered entity to the extent that the activities are related to covered functions:

- conducting quality assessment and improvement activities, including outcomes evaluation, development of clinical guidelines, case management, and care coordination;

- reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance and health plan performance; 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; training of non-health care professionals; accreditation; certification; licensing; and credentialing;

- underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits; and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care;

- conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

- business planning and development, such as conducting cost-management and planning related analyses relating to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies;

- business management and general administrative activities of the covered entity including, but not limited to: (i) management activities relating to implementation of and compliance with the requirements of the Privacy Standards; (ii) customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; (iii) resolution of internal grievances; (iv) the sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and (v) consistent with the applicable requirements of 45 C.F.R. § 164.514, creating de-identified health information and fundraising for the benefit of the covered entity.[17]

To the extent the OHCA needs protected health information maintained by any one member of the OHCA to carry out any one of these health care operations and such operations would benefit the common enterprise, the member that maintains the information may disclose the information for that purpose.

D. Only One "Joint Notice" Needs To Be Developed for the Entire OHCA.

The Privacy Standards provide that individuals have the right to receive an adequate notice of the uses and disclosures of PHI that may be made by a covered entity, and of the individual's rights and the covered entity's legal duties with respect to PHI. This requirement is set forth in detail at 45 C.F.R. § 164.520 and is called the "Notice of Privacy Practices" requirement or, more simply, just the "Notice" requirement. The Privacy Standards require certain covered entities to develop and issue their own Notices, and the Proposed Modifications additionally require covered health care providers who have a direct treatment relationship with their patients to make a good faith effort to obtain their patients' written acknowledgment of the patients' receipt of the Notice except in emergency treatment situations.[18]

Importantly, the Privacy Standards allow covered entities that participate in an OHCA to comply with the Notice requirement by producing a single "Joint Notice" that describes the members' combined privacy practices, if certain requirements are met.[19] Specifically:

- The covered entity members must agree to abide by the terms of the Joint Notice with respect to PHI created or received by the covered entities as part of their participation in the OHCA;

- The Joint Notice must reasonably identify the covered entities, or class of covered entities, to which the Joint Notice applies, and the service delivery sites, or classes of service delivery sites, to which the Joint Notice applies;

- If the covered entities participating in the OHCA will share PHI with each other as necessary to carry out treatment, payment, or health care operations relating to the arrangement, that fact must be stated in the Notice;[20] and

- The OHCA must document compliance with the Notice requirement by retaining a copy of the Joint Notice issued by the OHCA for six years from the date of the Notice's creation or the date when it last was in effect, whichever is later.[21]

The Privacy Standards make it easy for the covered entity members of the OHCA to satisfy the Joint Notice requirement by stating that if any one of the covered entity members of the OHCA provides the Joint Notice to a given individual, the distribution requirement with respect to that individual is met for all of the covered entities included in the Joint Notice.[22]

For example, a covered hospital and its attending physicians may elect to produce a Joint Notice. When an individual is first seen at the hospital, the hospital must provide the individual with a copy of the Joint Notice. Once the hospital has done so, the notice distribution requirement for all of the attending physicians that provide treatment to the individual at the hospital and that are included in the Joint Notice is satisfied.[23] The Joint Notice thus benefits each member of the OHCA because each member is not required to develop and issue its own Notice to each individual.

Please note that the preamble distinguishes between the Joint Notice requirements that apply to OHCAs (discussed above), and the single (but not Joint) Notice requirement that appears to apply to SACEs (discussed in more detail in Section IV(B), below):

> We note that, under § 164.504(d), covered entities that are under common ownership or control may designate themselves as a single affiliated covered entity. Joint notice requirements do not apply to covered entities that designate themselves as a single affiliated covered entity. Single affiliated covered entities must produce a single notice, consistent with the requirements for any other covered entity. Covered entities under common ownership or control that elect not to designate themselves as a single affiliated covered entity, however, may

elect to produce a joint notice if they meet the definition of an organized health care arrangement.[24]

E. Uses and Disclosures for the TPO of the OHCA Are Permitted Without Consent or Authorization.

As discussed in Section III(A), above, covered entities that participate in an OHCA and that have developed a Joint Notice may use and disclose PHI for any TPO activities of the OHCA without individual consent or authorization.[25]

F. Only One Privacy Official and One Contact Person Need To Be Designated for the Entire OHCA.

Covered entities are required to designate a privacy official who is responsible for the development and implementation of the privacy policies and procedures of the entity.[26] Covered entities also are required to designate a contact person or officer who is responsible for receiving complaints and who is able to provide further information about matters covered by the Notice.[27] The Privacy Standards collectively refer to the designation of the privacy official and the contact person as "personnel designations."

The preamble states that "[i]f several covered entities share a notice for services provided on the same premises, pursuant to § 164.520(d) [the section referring to covered entities that participate in an OHCA and issue a Joint Notice], that notice need designate only one privacy official and contact person for information collected under that notice." Thus, to the extent covered entities participate in an OHCA and issue a Joint Notice, the preamble appears to permit such covered entities to designate just one privacy official and one contact person for the information collected under that Joint Notice.[28] There is nothing in the HIPAA Privacy Standards that prohibits the privacy official and the contact person from being the same person.

IV. Single Affiliated Covered Entities

A. Covered Entities Under Common Ownership or Control May Designate Themselves as a SACE.

Legally separate[29] covered entities that are affiliated may treat themselves (including any health components of such covered entities)[30] as a single affiliated covered entity (or "SACE") for purposes of the Privacy Standards, if:

- all of the covered entities designated are under *common ownership or control*;[31]
- the designation of the SACE is documented and documentation of the designation is maintained in written or electronic form for six years from the date of its creation or the date when it last was in effect, whichever is later;[32]

- if the SACE performs multiple covered functions that would make the entity any combination of a health plan, health care provider, or a health care clearinghouse, the SACE must comply with all of the requirements, standards, and implementation specifications set forth in the Privacy Standards that apply to the health plan, heath care provider, or health care clearinghouse covered functions performed; and

- if the SACE combines the functions of a health plan or health care provider, the SACE may use or disclose the PHI of individuals who receive either the health plan or health care provider's services, but not both, only for purposes related to the appropriate function being formed.[33]

The only requirement that entities must meet *before* designating themselves as a SACE is discussed under the first bullet, above: that of common ownership or control. The Privacy Standards explain that *common ownership* exists when an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.[34] *Common control* exists when an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.[35]

The requirement discussed in the second bullet above simply obligates the members of the SACE to state in writing at the time of the SACE's designation: (i) the names of each of the affiliated entities that together make up the SACE; (ii) a description of how they are related through common ownership or control; and (iii) the fact that the entities are designating themselves as a single affiliated covered entity under 45 C.F.R. § 164.504(d). Then, the SACE must maintain that statement in written or electronic form for as long as the SACE is so designated plus six years.

The requirement discussed under the third bullet above basically provides that the requirements that apply to any one covered entity under the Privacy Standards also will apply to the entire SACE. Thus, under the minimum necessary provisions set forth in the Privacy Standards, a corporation with hospitals in 20 states may designate itself as a SACE, but one of the hospitals may not share PHI about a particular patient with another hospital if such use is not necessary for treatment, payment, or health care operations, and an authorization has not been obtained.[36] Stated another way, "transfers of information within the affiliated entity are uses, while transfers of information outside the affiliated entity are disclosures."[37] Moreover, if the SACE contains health components, it must implement safeguards to prevent the larger entity from using PHI maintained by the health component entity. (*See* Section VI(D) of this Legal Analysis for a discussion of the safeguard requirements that apply to health components.)

The requirement discussed under the fourth bullet, above, is best understood by reference to an example set forth in the preamble to the Privacy Standards: "a health care system may not share information about a patient in its hospital with its health plan if the patient is not a member of the health plan."[38] Thus, under the fourth bullet, to the extent the SACE includes entities that provide both health plan and health care provider services, the SACE may use or disclose the

PHI of individuals who receive one service, but not the other, only for a purpose relating to the service received.

Finally, although legally separate covered entities under common ownership or control may designate themselves as a SACE, the individual covered entities that together make up the SACE separately are subject to liability under the Privacy Standards.[39]

B. Only a Single Shared Notice Is Required for a SACE.

The preamble to the Privacy Standards states that single affiliated covered entities may promulgate a single shared Notice.[40] *See* 62 Fed. Reg. at 82637 ("Aggregation into a single covered entity will allow the entities to use a single notice of information practices . . . "); *id.* at 82725 ("An affiliated covered entity only is required to produce a single notice."). Thus, each member of the single affiliated entity does not have to produce its own Notice, but may rely on a shared Notice developed and issued by the SACE.

Again, please note that the preamble distinguishes between the Joint Notice requirements that apply to OHCAs (discussed above), and the single notice requirement that applies to SACES:

> Joint notice requirements do not apply to covered entities that designate themselves as a single affiliated covered entity. Single affiliated covered entities must produce a single notice, consistent with the requirements for any other covered entity. Covered entities under common ownership or control that elect not to designate themselves as a single affiliated covered entity, however, may elect to produce a joint notice if they meet the definition of an organized health care arrangement.[41]

C. Only One Privacy Official and One Contact Person Need Be Designated For the Entire SACE.

The preamble to the Privacy Standards explains that:

> The designation of privacy official and contact person positions within affiliated entities will depend on how the covered entity chooses to designate the covered entity(ies) under § 164.504(b). If a subsidiary is defined as a covered entity under this regulation, then a separate privacy official and contact person is required for that covered entity. *If several subsidiaries are designated as a single covered entity, pursuant to § 164.504(b), then together they need have only a single privacy officer and contact person*.

The preamble further states that:

> Comment: Some comments expressed concern that the regulation would require a company with subsidiaries to appoint a privacy official within each subsidiary.

> Instead they argued that the corporate entity should have the option of designating a single corporate official rather than one at each subsidiary.
>
> Response: In the final regulation, we give covered entities with multiple subsidiaries that meet the definition of covered entities under this rule the flexibility to designate whether such subsidiaries are each a separate covered entity or are together a single covered entity. (*See* § 164.504(b) for the rules requiring such designation.) If only one covered entity is designated for the subsidiaries, only one privacy officer is needed. Further, we do not prohibit the privacy official of one covered entity from serving as the privacy official of another covered entity, so long as all the requirements of this rule are met for each such covered entity.[42]

As stated above, there is nothing in the HIPAA Privacy Standards that prohibits the privacy official and the contact person from being the same person.

V. Application Issues Relating to OHCAs and SACEs

A. What Happens If a Covered Entity Conducts Business Both as Part of an OHCA or a SACE and as an Independent Enterprise?

A covered entity that conducts business both as part of an OHCA or SACE *and* as an independent enterprise (e.g., a physician who sees patients through an on-call arrangement with a hospital and through an independent private practice) may want to adopt different privacy practices with respect to each line of business. If this is the case, the Privacy Standards would require the covered entity to develop two different Notices because "covered entities must produce Notices that accurately describe the privacy practices that are relevant to the individuals receiving the Notice."[43]

Thus, to the extent a physician and a hospital meet the definition of an organized health care arrangement, the physician and the hospital may establish a Joint Notice that describes the privacy practices relating to protected health information created by the hospital or the physician and maintained at the hospital. When treating patients at the hospital, the physician may rely on that Joint Notice. However, with respect to patients who are treated at the physician's private clinic and whose PHI is maintained at the clinic, the physician must issue his or her own Notice describing his or her privacy practices at the clinic.

B. What Happens If Two or More Covered Entities Do Not Meet the Definition of an OHCA or a SACE Under the Privacy Standards?

Sometimes two or more covered entities will be somewhat related but they will not meet the definition of an OHCA or a SACE. For example, two covered entities may participate in some type of organized system of health care but they will not hold themselves out to the public as participating in a joint arrangement or will not participate in one of the three joint activities required to meet the definition of an OHCA. Or, two entities may be affiliated, but they are not exactly under common ownership or control, as would be required to meet the definition of a SACE.

The Privacy Standards explain that if two or more covered entities do not meet the definition of an OHCA or a SACE, then before one of the covered entities can disclose PHI to another covered entity for a non-TPO purpose, or for a health care operation activity not described in the first or second paragraph of the definition of health care operations or the purpose of which is not health care fraud and abuse detection or compliance, the first covered entity must obtain the patient's authorization in accordance with 45 C.F.R. § 164.508, *just as if the first entity was disclosing the PHI to a completely unrelated party*. The preamble explains that such an authorization may be useful to accomplish clinical coordination and integration among covered entities that do not meet the definition of an OHCA or a SACE. For example, safety-net providers that participate in the Community Access Program (or "CAP") may not qualify as an OHCA but may want to share PHI with each other in order to develop and expand integrated systems of care for uninsured people. An authorization would permit such providers to receive PHI from other CAP participants to engage in such activities.[44]

VI. Hybrid Entities

A. Really Generally–How the Privacy Standards Apply to Hybrid Entities.

The Privacy Standards establish the concept of a "hybrid entity" which, as amended by the Proposed Modifications, is defined as a single legal entity: (1) that is a covered entity; (2) whose business activities include both covered and non-covered functions; and (3) that appropriately designates health care components.[45]

Under the Proposed Modifications, covered entities that quality as a hybrid entity may choose whether or not they want to be hybrid entities.[46] With respect to covered entities that qualify as and choose to be hybrid entities, the Privacy Standards apply only to the part of the hybrid entity that is the health component.[47] At the same time, the lack of corporate boundaries between the health component and the other divisions (hereinafter, the "non-health components") increases the risk that PHI will be used in a manner that would not otherwise be permitted by the Privacy Standards. Thus, the Privacy Standards require the legal entity to be responsible for ensuring that the health component complies with the Privacy Standards with respect to any PHI, and to erect firewalls to protect against the improper use or disclosure of PHI within or by the organization.[48] To avoid needless application of the hybrid entity provisions to a covered entity's activities as an employer, the Proposed Modifications amend the definition of PHI to clarify that employment records are not PHI. Specifically, the Proposed Modifications expressly exclude employment records held by a covered entity in its role as employer from the definition of PHI.[49] This change limits the need for a covered entity whose primary activities are covered functions to designate itself as a hybrid entity simply to carve out employment records.[50]

B. Is Your Organization a Hybrid Entity?

As discussed above, the amended Privacy Standards specifically define a hybrid entity as a *single legal entity*: (1) that is a covered entity; (2) whose business activities include both *covered and non-covered functions*; and (3) that appropriately *designates health care components*.[51]

1. "Single Legal Entity."

The Privacy Standards define a "single legal entity" as a legal entity, such as a corporation or partnership, that cannot be further differentiated into units with their own legal identities.[52] For example, a multinational corporation composed of multiple subsidiary companies would not be a single legal entity, because the multinational corporation can be further differentiated into subsidiary units that have their own legal identities. However, a small manufacturing firm and its health clinic, if the health clinic is not separately incorporated, could be a single legal entity.[53] Or, a law firm that is organized as a limited liability partnership and that self administers a group health plan, could be a single legal entity.

2. "Covered and Non-Covered Functions."

The Proposed Modifications require single legal entities who wish to qualify as a hybrid entity to have business activities that include both *covered and non-covered functions*. The Privacy Standards explained that *covered functions* are a shorthand way of expressing the functions performed by health plans (e.g., providing, or paying for, the cost of medical care), health care providers (e.g., furnishing health care services or supplies), and health care clearinghouses (e.g., processing or facilitating the processing of data elements of health information).[54]

The term "covered functions" is not intended to include various support functions, such as computer support, payroll and other office support, and similar support functions, although the Privacy Standards recognize that these support functions must occur in order for the entity to carry out its covered functions. Because such support functions often are also performed for the parts of the organization that are not doing covered functions, the Privacy Standards require the workforce who perform these support functions to not impermissibly use or disclose PHI.[55]

3. Designation of Health Components.

Finally, a single legal entity that otherwise qualifies as a hybrid entity must designate a component or combination of components as its *health components* in accordance with amended 45 C.F.R. § 164.504(c)(3)(iii). Specifically, the Proposed Modifications explain that the covered entity is responsible for designating the components that are part of one or more health components of the covered entity and documenting the designation.[56] The Proposed Modifications further explain that if the covered entity designates a health component or components, it must include any component that would meet the definition of a covered entity if it were a separate legal entity.[57]

The Proposed Modifications further explain that health component(s) *may* include a component that performs: (1) covered functions; and (2) activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.[58] The Proposed Modifications emphasize that a covered entity may, but is not required to, include in its health component designation components that engage in "business associate" functions in its health component.[59] The preamble specifically states that it is not a violation of the Privacy Standards to fail to include

such a component in the health component designation. However, a disclosure of PHI from the health component to such other component if it is not part of the health component is the same as a disclosure outside the covered entity and is a violation unless it is permitted by the Privacy Standards. Because an entity cannot have a business associate agreement with itself, such a disclosure likely would require individual authorization.[60]

Commenters to the final Privacy Standards had expressed concern regarding whether a component of a covered entity that is a provider, but that does not conduct standard electronic transactions, should be included in the health component. The Proposed Modifications explain that a component that is a health care provider and that engages in standard electronic transactions *must be included in the health component*, but a component that is a health care provider but that does not engage in standard electronic transactions *may, but would not be required to*, be included in the health component of the hybrid entity. The decision would be left to the covered entity in the second situation.[61]

For example, the preamble explains that in a university setting, the single legal entity may operate hospital facilities that bill electronically and research laboratories that do not engage in any electronic billing. The university as a hybrid entity need only include the hospital facilities that bill electronically in the health component; the university has the option to include the components, such as the research laboratory, that function as a health care provider, but not as a *covered* health care provider. A covered entity that chooses to include a non-covered health care provider in its health component would be required to ensure that the non-covered health care provider, as well as the rest of the health component, is in compliance with the Privacy Standards.

4. No More "Primary Functions" Determinations.

Under the *un*modified Privacy Standards, a legal entity was a hybrid entity only if its covered functions were not its "primary functions." If the covered functions performed were the organization's primary functions, the Privacy Standards would apply to the entire legal entity.

The Proposed Modifications delete the term "primary" from the definition of "hybrid entity." The preamble to the Proposed Modifications explains that:

> In order to avoid the problem of line drawing, the Department proposes to permit any covered entity to be a hybrid entity if it is a single legal entity that performs both covered and non-covered functions, regardless of whether the non-covered functions represents that entity's primary function, a substantial function, or even a small portion of the entity's activities.[62]

The Proposed Modifications further explain that elimination of the requirement in the definition of "hybrid entity" that covered functions not be the "primary" functions of the covered entity will greatly increase the proportion of covered entities that are hybrid entities. In order to avoid the burden of requiring many more covered entities to designate the health components and create fire walls within their entity when it is administratively simpler to treat the entire entity as a covered entity, the Proposed Modifications would allow the covered entity to choose whether it

will be a hybrid entity or not.[63] To accomplish this objective, a covered entity that otherwise qualifies as a hybrid entity must designate health care components. If a covered entity does not designate health care components, the entire entity would be a covered entity.[64]

C. What is the General Rule With Respect to Hybrid Entities?

Once you have determined that your organization qualifies as a hybrid entity and you have chosen to identify your organization as a hybrid entity by designating (and documenting the designation of) your health component(s), the next step is to determine how the Privacy Standards apply to hybrid entities. The general rule under the Privacy Standards with respect to hybrid entities is that the Privacy Standards only apply to the health component of the hybrid entity.[65] This means that any reference in the Privacy Standards to a "covered entity" actually is to the health component of the hybrid entity.[66] Moreover, any reference in the Privacy Standards to a "health plan," "covered health care provider," or "health care clearinghouse" actually is to the health component of a hybrid entity that performs the function of a health plan, health care provider, or health care clearinghouse, as appropriate.[67] Finally, any reference to "protected health information" in the Privacy Standards actually is to protected health information that is created by or received by or on behalf of a health component of a hybrid entity. Thus, to the extent that your organization is a hybrid entity, you should read the Privacy Standards with these "translations" in mind.

D. What Kind of Safeguards Must Hybrid Entities Establish To Prevent the Hybrid Entity's Non-Health Components from Inappropriately Accessing Protected Health Information?

The Privacy Standards, at 45 C.F.R. § 164.504(c)(2), require hybrid entities with a health component to establish safeguard policies and procedures to prevent any access to PHI by its other organizational units that would not be otherwise permitted by the Privacy Standards.[68] The HIPAA statute itself requires policies and procedures to isolate the activities of a health care clearinghouse from a "larger organization" to prevent unauthorized access by the larger organization.[69] Thus, the safeguard provision set forth in the Privacy Standards is consistent with the statutory requirement and extends to any hybrid entity that performs "non-covered entity functions" or operates or conducts functions of more than one type of covered entity.[70]

The Privacy Standards explain that the safeguard requirements are necessary to provide meaningful privacy protections, particularly because the health component is part of a larger legal organization that performs functions other than those covered under the Privacy Standards.[71] Without the safeguard requirement the Privacy Standards cannot ensure that the health component will not share PHI with the larger entity.

Interestingly, the Privacy Standards do not specifically identify the safeguards that are required; however, the Privacy Standards do explain that the covered entity must implement policies and procedures to ensure that:

> The health component's use and disclosure of PHI complies with the Privacy Standards. This means that the health component must not disclose PHI to a non-

health component of the covered entity if the Privacy Standards would prohibit the disclosure if the health component and the non-health component were separate and distinct legal entities.[72]

Members of the health component who perform duties for the larger entity do not use and disclose PHI obtained through the health component while performing non-health component functions unless otherwise permitted or required by the Privacy Standards. Thus, if a person performs duties for both the health component and for a non-health component of the entity in the same capacity, the person must not use or disclose PHI created or received in the course of or incident to the member's work for the health component in a way prohibited by the Privacy Standards.[73]

When a covered entity conducts multiple covered functions, the health component adheres to the appropriate requirements (e.g., when acting as a health plan, adheres to the health plan requirements) and uses or discloses PHI of individuals who receive limited functions from the component only for the appropriate functions.[74] *Thus, for example, a covered entity that includes both a hospital and a health plan may not use PHI obtained from an individual's hospitalization for the health plan, unless the individual also is enrolled in the health plan. (As an exception, however, covered entities always are permitted to make a disclosure to a health care provider for treatment of an individual without restrictions)*.

E. What About "Excepted Benefits?"

The Privacy Standards generally define "health plan" to include an individual or group plan that provides, or pays the cost of, *medical care*.[75] The Privacy Standards specifically except from the definition of "health plan" any policy, plan, or program to the extent that it provides, or pays for the cost of, the following "excepted benefits":

- Coverage only for accident, or disability income insurance, or any combination thereof.
- Coverage issued as a supplement to liability insurance.
- Liability insurance, including general liability insurance and automobile liability insurance.
- Workers' compensation or similar insurance.
- Automobile medical payment insurance.
- Credit-only insurance.
- Coverage for on-site medical clinics.

- Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.[76]

These "excepted benefit programs" or "excepted benefits" are programs that, by definition, cannot be part of a health component of a hybrid entity. Accordingly, to the extent a hybrid entity has a component that performs the functions of a "health plan," as well as components that perform the function of one of the above listed "excepted plans," the hybrid entity must treat the "excepted plans" component as a non-health component.

F. Who Is Ultimately Responsible for Ensuring Compliance with the Privacy Standards?

The Privacy Standards state that the covered entity in the hybrid entity situation is the legal entity itself, not just the health component of the legal entity. Thus, the entire hybrid legal entity is the entity that is responsible for ensuring that the health components comply with the Privacy Standards. The Privacy Standards reason that the legal entity has control over the entire workforce, not just the workforce of the health component. Thus, the legal entity is in the position to implement policies and procedures to ensure that the part of its workforce that is doing mixed or non-covered functions does not impermissibly use or disclose protected health information.[77] The Privacy Standards also require the hybrid entity to be responsible for designating the health components of the hybrid entity, documenting the designation, and maintaining the designation in written or electronic form for six years from the date of its creation or the date when the designation was last in effect, whichever is later.[78]

VII. Conclusion

The Privacy Standards apply specially to OHCAs, SACEs, and hybrid entities. Arrangements that meet the definition of an OHCA may share PHI for any TPO activity of the common enterprise without individual consent or authorization. In addition, affiliated covered entities under common ownership or control may designate themselves as a SACE, and transfers of PHI within the single affiliated covered entity for any TPO activity are considered permitted uses. Finally, the Privacy Standards technically only apply to the health components of hybrid entities, although the hybrid entity is legally responsible for ensuring that its health components do not impermissibly use or disclose protected health information, and that its non-health components do not impermissibly access protected health information.

See the two attachments that chart a decision tree to aid in determining if an entity is an "OHCA" or a "SACE [**Attachment 1**] or a hybrid entity [**Attachment 2**].

886102_1.DOC

Where HHS has proposed to amend a regulatory reference, the reference is followed by the following notation: "(as amended by the Proposed Modifications)."

[1] 65 Fed. Reg. 82462 (Dec. 28, 2000).

[2] 67 Fed. Reg. 14776 (Mar. 27, 2002).
[3] 65 Fed. Reg. at 82494.
[4] The standard transactions are set forth at 65 Fed. Reg. 50312 (August 17, 2000).
[5] 45 C.F.R. § 164.506(c)(2) (as amended by the Proposed Modifications).
[6] 45 C.F.R. § 164.506(c)(3) (as amended by the Proposed Modifications).
[7] 45 C.F.R. § 164.506(c)(4) (as amended by the Proposed Modifications).
[8] 65 Fed. Reg. at 82494, 82725.
[9] 65 Fed. Reg. at 82494.
[10] 65 Fed. Reg. at 82494.
[11] 65 Fed. Reg. at 82494.
[12] 65 Fed. Reg. at 82804.
[13] 65 Fed. Reg. at 82494-95.
[14] 65 Fed. Reg. at 82476. Please note that the fact that two or more covered entities participate in an organized health care arrangement does not make any of the covered entities a business associate of the other covered entity. Moreover, the fact that the entities participate in a joint health care operations or other joint activities, or pursue common goals through a joint activity, does not mean that one party is performing a function or activity on behalf of the other party.
[15] 65 Fed. Reg. at 82803-04; 45 C.F.R. § 164.501.
[16] 45 C.F.R. § 164.506(c)(5) (as amended by the Proposed Modifications).
[17] 45 C.F.R. § 164.501 (definition of health care operations) (as amended by the Proposed Modifications).
[18] *See* 45 C.F.R. § 164.520(b)(1) and 45 C.F.R. § 164.520(c)(2)(ii) (as amended by the Proposed Modifications).
[19] 65 Fed. Reg. at 82552, 82725.
[20] 65 Fed. Reg. at 82552.
[21] 65 Fed. Reg. at 82822.
[22] 65 Fed. Reg. at 82725.
[23] 65 Fed. Reg. at 82725. The preamble explains that covered health care providers that have an indirect treatment relationships with individuals, such as clinical laboratories, and, thus, only are required to provide the notice upon request, may elect to reach agreements with other entities who can distribute their notice on their behalf, or can participate in an OHCA that produces a Joint Notice.
[24] 65 Fed. Reg. at 82552.
[25] 45 C.F.R. § 164.506(c)(5) (as amended by the Proposed Modifications).
[26] 65 Fed. Reg. at 82826; 45 C.F.R. § 164.530(a)(1)(i).
[27] 65 Fed. Reg at 82826; 45 C.F.R. § 164.530(a)(1)(ii).
[28] 65 Fed. Reg. at 82561 (bracketed language added).
[29] A "single legal entity" is defined as a legal entity, such as a corporation or partnership, that cannot be further differentiated into units with their own legal identities. 65 Fed. Reg. at 82502.
[30] A complex organization, depending on how it self-designates, may have one or several "health care component(s)" that are each a covered entity. 65 Fed. Reg. at 82637. *See* Section VI of this Legal Analysis.
[31] Common ownership is defined as an ownership or equity interest of five percent or more. 65 Fed. Reg. at 82638. Common control exists if an entity has the power–directly or indirectly–significantly to influence or direct the actions or policies of another entity. *Id.*
[32] 45 C.F.R. §§ 164.530(j)(1)(iii), 164.530(j)(2).
[33] 45 C.F.R. §§ 164.504(d), 164.504(g).
[34] 45 C.F.R. § 164.504(a).
[35] 45 C.F.R. § 164.504(a).
[36] 65 Fed. Reg. at 82503.
[37] 65 Fed. Reg. at 82607.
[38] 65 Fed. Reg. at 82509.
[39] 65 Fed. Reg. at 82503.
[40] 65 Fed. Reg. at 82503.
[41] 65 Fed. Reg. at 82552.
[42] 65 Fed. Reg. at 82745 (bolded emphasis added). Although the sections quoted above cite to § 164.504(b), not § 164.504(d) (which is the provision giving permission to covered entities under common ownership or control to

designate themselves as a single affiliated covered entity), the sections quoted above suggest that if covered entities under common ownership or control designate themselves as a single affiliated covered entity, that affiliated entity need only have one privacy officer and one contact person.

[43] 65 Fed. Reg. at 82548.
[44] 65 Fed. Reg. at 82519.
[45] 45 C.F.R. § 164.504(a) (as amended by the Proposed Modifications).
[46] 67 Fed. Reg. at 14803.
[47] 45 C.F.R. § 164.504(c)(1)(ii).
[48] 65 Fed. Reg. at 82502; 45 C.F.R. § 164.504(c)(2).
[49] 67 Fed. Reg. at 14804; 45 C.F.R. § 164.501 (definition of PHI) (as amended by the Proposed Modifications). The preamble to the Proposed Modifications clarify that the exception from the definition of PHI for employment records only applies to individually identifiable health information in those records that are held by a covered entity in its role as employer. The exception does not apply to individually identifiable health information held by a covered entity when carrying out its health plan or health care provider functions; such information is PHI. HHS is soliciting comments regarding whether the term "employment records" is clear or whether it needs to be more fully explained. 67 Fed. Reg. at 14804.
[50] 67 Fed. Reg. at 14804.
[51] 45 C.F.R. § 164.504(a) (as amended by the Proposed Modifications).
[52] 65 Fed. Reg. at 82502.
[53] 65 Fed. Reg. at 82502.
[54] 65 Fed. Reg. at 82489.
[55] 65 Fed. Reg. at 82489.
[56] 45 C.F.R. § 164.504(c)(3)(iii) (as amended by the Proposed Modifications).
[57] 45 C.F.R. § 164.504(c)(3)(iii) (as amended by the Proposed Modifications).
[58] 45 C.F.R. § 164.504(c)(3)(iii)(A), (B) (as amended by the Proposed Modifications).
[59] 67 Fed. Reg. at 14804.
[60] 67 Fed. Reg. at 14804.
[61] 67 Fed. Reg. at 14803.
[62] 67 Fed. Reg. at 14803.
[63] 67 Fed. Reg. at 14803.
[64] 67 Fed. Reg. at 14803.
[65] 45 C.F.R. § 164.504(b).
[66] 45 C.F.R. § 164.504(c)(1)(i).
[67] 45 C.F.R. § 164.504(c)(1)(ii) (as amended by the Proposed Modifications).
[68] 65 Fed. Reg. at 82503.
[69] HIPAA § 1173(d)(1)(B).
[70] 65 Fed. Reg. at 82503.
[71] 65 Fed. Reg. at 82638.
[72] 45 C.F.R. § 164.504(c)(2)(i).
[73] 45 C.F.R. § 164.504(c)(2)(iii).
[74] 65 Fed. Reg. at 82638 (*citing* 45 C.F.R. §§ 164.504(c)(2), 164.504(g)).
[75] 45 C.F.R. § 160.103.
[76] 45 C.F.R. § 160.103 (excluding from the definition of health plan any policy, plan, or program to the extent that it provides, or pays for the cost of, the excepted benefits that are listed at listed at 42 U.S.C. § 300gg-91(c)(1) (Section 2791(c)(1) of the Public Health Service Act)).
[77] 65 Fed. Reg. at 82503 (*citing* 45 C.F.R. § 164.504(c)(3)(ii)).
[78] 45 C.F.R. § 164.504(c)(3)(ii), (iii).

