



Director
Office for Civil Rights
Washington, D.C. 20201

SEP 3 2004

Ms. Suellen R. Galbraith
Director for Public Policy
ANCOR
1101 King Street, Suite 380
Alexandria, Virginia 22314

Mr. Robert M. Gettings
Executive Director
NASDDDS
113 Oronoco Street
Alexandria, Virginia 22314

Transaction Number: 03-10790

Dear Ms. *Suellen and Bob:* Galbraith and Mr. Gettings:

Thank you for your thoughtful letter regarding the health information privacy regulation (Privacy Rule) issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and its application to providers of supports and services to individuals with mental retardation and other disabilities, as well as state agencies charged with developing service delivery systems that furnish supports to people with developmental disabilities.

I have appreciated the opportunities we have had to discuss these and other issues with you at our meeting in April 2003, at various subsequent events, and the interaction of the professionals from your respective organizations with OCR; as we work together to help your members understand how the Privacy Rule applies in their varied contexts. I trust that this letter, which we believe responds to most of the issues your letter raises, will further those ends, as we continue to work together to ensure that those served by your organizations will receive the rights to which they are entitled under the Privacy Rule in a way that does not impede access to quality care.

Covered Entity Status

A number of issues you have raised relate to the threshold inquiry regarding when an organization is a "covered entity" that is subject to the requirements of the Privacy Rule; seeking to clarify whether providers of supports and services that are paid for by Medicaid or pursuant to a Medicaid home and community-based services (HCBS) waiver are covered entities. As helpful

information that is available on the Department's website explains,¹ the Privacy Rule subjects the following types of entities to the HIPAA Administrative Simplification regulations, including the Privacy Rule: health plans, health care clearinghouses, health care providers who transmit any health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted a standard, and sponsors of a Medicare-endorsed prescription drug discount card. Whether a particular organization is a covered entity depends upon specific facts related to the entity's operations, rather than on the source of its funding. Specifically, whether an entity is a health care provider depends on whether the services or support it provides constitutes "health care", as defined in the Rule, and whether it transmits health information in electronic form in connection with a transaction for which the Department has adopted Standards. As such, knowing that an organization receives Medicaid funding is insufficient to determine whether it is a HIPAA-covered entity.

This question and your question whether all Medicaid supports and services or all Medicaid home and community-based waiver (HCBS) program services are considered "health care" for HIPAA purposes, were addressed, at least in part, by the March 21, 2002 letter from CMS to Phyllis J. Dube, Secretary of the Department of Health and Family Services for the State of Wisconsin (CMS letter), of which you both are aware. As that letter indicates, some services that may be provided under Medicaid or HCBS waivers, as "medical assistance", will clearly not be considered "health care" for HIPAA purposes, e.g., non-medical transportation, home and vehicle modifications, homemaker services, personal care services, habilitation and respite services. Other services or supplies will clearly qualify as health care services, e.g., clinical services to mentally ill individuals, dental services, pharmacy items, physical therapy, audiology services.

The Social Security Act defines the term "medical assistance" as the payment for the costs of enumerated categories that are basic to the Medicaid program. SSA §1905(a), 42 U.S.C. 1396d. The HIPAA regulations define health care to mean, "care, services, or supplies related to the health of an individual." It includes, but is not limited to, "(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription." 45 CFR §160.103. While there may be overlap between these two definitions, they are not identical; and as stated above, the funding source does not determine status as a covered entity.² Further, as you well know,

¹See the OCR website, <http://www.hhs.gov/ocr/hipaa/>, for a link to the decision tool, "Am I a Covered Entity?", and numerous other educational materials, including fact sheets and FAQs, that assist in understanding the Privacy Rule and HIPAA.

²For instance, we understand that individual state Medicaid agencies, in partnership with CMS, have designed waiver programs that allow individuals to choose alternative mechanisms that will provide supports and services, such as in consumer-directed initiatives. This allows

Medicaid policies for services are complex and vary from state to state: each of the fifty States, the District of Columbia and the Territories determines important elements of the type and scope of the Medicaid program services it provides. Moreover, at least eighty-one HCBS waiver programs are currently operative. Because application of the HIPAA Privacy Rule to a particular organization depends on such varying facts and circumstances, we are unable to define with greater specificity at this time how the Rule would apply to a particular program or service.

Notice of Privacy Practices

You also inquired whether residential and vocational providers who are under contract with the state (such as state Medicaid and/or MR/DD agencies) are required to post both their own Notice of Privacy Practices as well as the Notice of Privacy Practices provided by the State. At the outset, we note that State Medicaid agencies are health plans, and thus are not typically required to post a Notice of Privacy Practices. Further, as stated above, an MR/DD agency may or may not be a covered health care provider under the Privacy Rule. However, under the Rule, a covered health care provider who is a direct treatment provider is required to post its Notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered provider to be able to read the Notice, 45 CFR §164.520(c)(2), and the Notice must be posted at each physical service delivery site. It is conceivable that a State, operating as a covered health care provider, may have satellite offices operated by contracted private entities, and that as such, the State would require these private entities to apply the State's privacy practices, including providing and posting the State's Notice. In that event, a residential or vocational provider which is itself a covered entity subject to a Notice requirement, may elect to develop a joint Notice with the State, provided the Notice accurately reflects both entities' privacy policies.

Business Associates

Some of the inquiries you raised concern business associate relationships, including when a business associate relationship with a covered entity arises, and the nature of the respective responsibilities of these entities. Under the Privacy Rule a business associate provides a function or service to a covered entity that involves the use or disclosure of individually identifiable health information other than as a member of the workforce of the covered entity. 45 CFR §160.103. ("Workforce" is also a term defined in the Rule). To the extent that such an entity or vendor is merely selling or providing a product or service to a covered entity, but not otherwise performing a function or activity on behalf of the covered entity or providing services to or for the covered entity that involves the entity's use or disclosure of protected health information, the entity is not functioning in the capacity of a business associate. On the other hand, when an entity is a

individuals with disabilities in waiver programs to have more direct control over the supports and services they receive. The fact that such supports and services may be consumer-directed will not of itself determine whether such supports and services are health care as defined in the Privacy Rule; and if an entity satisfies the definition of a covered health care provider under the Rule, the fact that the services are delivered under the traditional Medicaid program or under a HCBS waiver will not affect its status as a covered entity.

business associate of a covered entity, the Rule requires that the covered entity contractually obligate the business associate to appropriately protect any health information the business associate may receive from the covered entity.³ Finally, even a covered entity may be a business associate of another covered entity, in which case that business associate will be obligated to comply with the Rule's requirements incumbent on it as a covered entity.

No Specific HIPAA Exemptions for MR/DD Providers

Related to the first question above, you have asked whether the HIPAA statute or accompanying regulations specifically exempt MR/DD providers from compliance with the regulations. As discussed previously, the Rule looks to the functions an organization performs to determine whether it is a covered entity, and does not expressly exempt MR/DD providers.

Interaction of FERPA and HIPAA

Both the U.S. Department of Health and Human Services (HHS) and the U.S. Department of Education (DOE) have clarified that education records covered by FERPA – the Family Education Rights and Privacy Act – are excluded from the HIPAA definition of protected health information, and as such, are not subject to the Privacy Rule. See 45 CFR §160.103. Thus, when educational records are covered by FERPA, a student's health information which may be contained in those records is subject to the protections Congress enacted under that act, rather than subject to Privacy Rule protections (see 65 Fed.Reg. 82483 and 69 Fed.Reg. 21672). To the extent records are not subject to FERPA and thus are covered by the Privacy Rule, a provider who is subject to the Rule must abide by the Privacy Rule protections on disclosure of protected health information to other third parties, including schools, and of course may also disclose this information as permitted by the Rule. For instance, a disclosure by a covered entity for its own treatment purposes, or for the treatment activities of another health care provider, is permitted by the Rule without patient authorization, 45 CFR §164.506(c)(1) and (2). As such, for example, the Rule permits disclosure of protected health information by a covered entity to a school nurse who is providing treatment to a student.

State Authorities and HIPAA

You inquired whether, or to what extent, State agencies may be delegated the authority or otherwise may have responsibility to promote compliance with the Privacy Rule. Neither HIPAA nor the Privacy Rule provides for delegation of the federal government's enforcement authority to a State, whether for civil enforcement activities over which OCR has authority, or criminal enforcement activities which Congress delegated to the U.S. Department of Justice. However, we are aware that many State and voluntary consortia have developed to assist covered entities in complying with the HIPAA Privacy Rule, and have developed helpful public information toward that end. While not endorsing specific projects, the Department supports voluntary activities to promote compliance with the Privacy Rule.

³See helpful guidance materials on business associates, including the Fact Sheet and numerous FAQs on this topic, available at the OCR website, www.hhs.gov/ocr/hipaa.

Involvement of Others on Behalf of MR/DD Population

You also inquired about communications between agencies and other providers which serve individuals with limited capacity to represent their own interests, including adult individuals with mental retardation, developmental disabilities or other disabilities. You point out that such individuals traditionally have relied on family members and friends to assist in communicating their interests even when the family member or friend has not formally been named as a legal representative or guardian of the individual. We recognize the importance of communication between covered entities and those who are legally responsible for care of the individual, or who otherwise may be involved in the care. The Privacy Rule is carefully balanced to permit disclosures to such persons for appropriate reasons and in appropriate contexts. For instance, unless the individual objects, the Privacy Rule generally allows health care providers and health plans to speak or otherwise share information about a patient's treatment or payment for health care with spouses, other family members, close personal friends, or any other persons identified by a patient as directly involved in that individual's care or payment for care. Under 45 CFR §164.510, the section that deals with these disclosures, a doctor or other health care provider covered by the Privacy Rule, or a health plan, may disclose information to a family member or friend if the individual is present and agrees or, given the opportunity, does not object to the disclosure; or the doctor or plan reasonably infers from the circumstances, based on professional judgment, that the patient does not object. For example, if a patient brings a friend to a medical appointment and asks if the friend may come into the treatment room, the doctor may reasonably infer that the patient does not object. Under these circumstances, a doctor or plan may disclose any information that is directly relevant to the family member, friend or other identified person involved with the patient's care, or payment related to the individual's care.

Even if the patient is not present or is incapacitated, a health care provider that is covered by the Privacy Rule can still disclose patient information directly related to the person's involvement with the individual's health care as long as, in the exercise of reasonable judgment, the provider determines that doing so would be in the best interest of the patient. In fact, the Privacy Rule expressly states that a covered entity such as a doctor or pharmacist can use professional judgment and experience with common reasonable inferences about the patient's best interests in allowing another person to act on behalf of the patient to pick up a filled prescription, medical supplies, X-rays, or other similar forms of protected health information. OCR's website offers a great deal of helpful guidance in this area.

Legal Guardians

You inquired whether a covered entity may disclose any and all protected health information to a guardian who was appointed as personal representative for a particular purpose only.

Generally, HIPAA and the Privacy Rule do not change how State laws affect the legal relationship and responsibilities relating to consent, legal capacity, or the exercise of such legal rights. Under the Privacy Rule, a person or entity that meets the HIPAA definition of a "personal representative" generally has a right to access the individual's health information as necessary to make health care decisions, within the scope of their legal authority to do so. The Rule defines a

“personal representative” as one who has health care decision making authority for an individual under state or other law. Thus, if a guardian, under State law, has broad authority (such as to make any and all health care decisions on behalf of an individual) then, except in certain limited circumstances defined in the Privacy Rule, the guardian similarly would have the right to broad access to that individual’s health information. On the other hand, if the guardian’s authority to make medical decisions is limited, for instance, to dietary decisions, then the guardian would have a right to access such health information as necessary to make informed decisions about the individual’s dietary needs. The enclosed Fact Sheet on “Personal Representatives” provides a helpful explanation of how, under the Privacy Rule, personal representatives are authorized to access health information on behalf of others.

Atypical, Non-medical Services.

You inquired whether atypical, non-medical services are considered “treatment” under the Privacy Rule, or are providers and payers required to obtain an individual’s authorization before individually identifiable health information can be used or disclosed.

As you point out, the preamble for the Transactions Rule clarifies that providers of non-medical services, such as homemaking or carpentry services, are not considered health care providers for claim and reimbursement purposes. We note, however, that page 50316 of the Transactions Rule preamble references “[t]hose atypical services that meet the definition of health care,” and thus recognizes that some atypical service providers may be health care providers, and covered health care providers. Some services reimbursable under Medicaid are within the definition of “health care” and some such services are not.

The term, “treatment” is defined more broadly than the term “health care” but, like “health care”, it is a term that cannot be defined by reference to an all-inclusive list of care, services, and supplies. Whether or not the atypical, non-medical services are considered treatment, is not necessarily determinative of the issue as to whether providers and payers are required to obtain an authorization before protected health information may be used or disclosed.

Whether protected health information may be used or disclosed by a provider or payer depends on the purpose for such use or disclosure. Disclosures for treatment purposes are permissible under the Privacy Rule as are disclosures for other, specified purposes in accordance with the Rule. For instance, the Privacy Rule permits a covered entity to use or disclose protected health information as needed for its own payment purposes. Moreover, a covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information. The term payment is defined in the Rule to include the activities of *a health plan to obtain premiums or to determine or fulfill its responsibilities for coverage and provision of benefits under the health plan*; and the activities of a health care provider or health plan to obtain or provide reimbursement for the provision of health care, 45 C.F.R. §164.501(1) (emphasis added). Thus, the Privacy Rule defines payment broadly enough to encompass certain disclosures from a health plan to an atypical service provider. Also, we note that depending upon the particular facts and circumstances, disclosures

Page 7 - Ms. Galbraith and Mr. Gettings


may also be permitted under 45 CFR §164.510(b)(1), concerning disclosures to any person whom the individual identifies as involved in his or her care, in accordance with the terms of that section.

Finally, of course, an authorization that complies with 45 CFR 164.508 executed by the individual or, where appropriate, the individual's personal representative, is sufficient to permit a covered entity to disclose health information.

* * * * *

I trust that the information contained in this letter, and the other exchanges we have had regarding the Privacy Rule, have been helpful to you and your members. We recognize that application in many of the settings in which services are provided to mentally retarded and developmentally disabled persons present circumstances that require careful consideration in applying the Privacy Rule, and that as we have reviewed many of these questions, we have discovered additional areas where further clarification may yet be helpful. Please be assured that we will continue our efforts to develop guidance as appropriate so that the Rule is understood and applied in a workable fashion, and that the twin goals of the Privacy Rule – assuring the protection of health information, while permitting access to quality care to continue – are fully achieved.

Please contact me if we can be of further assistance.

Sincerely,

Richard M. Campanelli, J.D.
Director

Enclosure

PERSONAL REPRESENTATIVES

[45 CFR 164.502(g)]

Background

The HIPAA Privacy Rule establishes a foundation of Federally-protected rights which permit individuals to control certain uses and disclosures of their protected health information. Along with these rights, the Privacy Rule provides individuals with the ability to access and amend this information, and the right to an accounting of certain disclosures. The Department recognizes that there may be times when individuals are legally or otherwise incapable of exercising their rights, or simply choose to designate another to act on their behalf with respect to these rights. Under the Rule, a person authorized (under State or other applicable law, e.g., tribal or military law) to act on behalf of the individual in making health care related decisions is the individual's "personal representative." Section 164.502(g) provides when, and to what extent, the personal representative must be treated as the individual for purposes of the Rule. In addition to these formal designations of a personal representative, the Rule at 45 CFR 164.510(b) addresses situations in which persons are involved in the individual's health care but are not expressly authorized to act on the individual's behalf.

How the Rule Works

General Provisions. Except as otherwise provided in 45 CFR 164.502(g), the Privacy Rule requires covered entities to treat an individual's personal representative as the individual with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule.

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. For instance, covered entities must provide the individual's personal representative with an accounting of disclosures in accordance with 45 CFR 164.528, as well as provide the personal representative access to the individual's protected health information in accordance with 45 CFR 164.524 to the extent such information is relevant to such representation. In addition to exercising the individual's rights under the Rule, a personal representative may also authorize disclosures of the individual's protected health information.

In general, the scope of the personal representative's authority to act for the individual under the Privacy Rule derives from his or her authority under applicable law to make health care decisions for the individual. Where the person has broad authority to act on the behalf of a living individual in making decisions related to health care, such as a parent with respect to a minor child or a legal guardian of a mentally incompetent adult, the covered entity must treat the personal representative as the individual for all purposes under the Rule, unless an exception

applies. (See below with respect to abuse, neglect or endangerment situations, and the application of State law in the context of parents and minors). Where the authority to act for the individual is limited or specific to particular health care decisions, the personal representative is to be treated as the individual only with respect to protected health information that is relevant to the representation. For example, a person with an individual's limited health care power of attorney regarding only a specific treatment, such as use of artificial life support, is that individual's personal representative only with respect to protected health information that relates to that health care decision. The covered entity should not treat that person as the individual for other purposes, such as to sign an authorization for the disclosure of protected health information for marketing purposes. Finally, where the person has authority to act on the behalf of a deceased individual or his estate, which does not have to include the authority to make decisions related to health care, the covered entity must treat the personal representative as the individual for all purposes under the Rule. State or other law should be consulted to determine the authority of the personal representative to receive or access the individual's protected health information.

Who Must Be Recognized as the Individual's Personal Representative. The following chart displays who must be recognized as the personal representative for a category of individuals:

If the Individual Is:

An Adult or
An Emancipated Minor

An Unemancipated Minor

Deceased

The Personal Representative Is:

A person with legal authority to make health care decisions on behalf of the individual

Examples: Health care power of attorney
Court appointed legal guardian
General power of attorney

A parent, guardian, or other person acting *in loco parentis* with legal authority to make health care decisions on behalf of the minor child

Exceptions: See parents and minors discussion below.

A person with legal authority to act on behalf of the decedent or the estate (not restricted to health care decisions)

Examples: Executor of the estate
Next of kin or other family member

Durable power of attorney

Parents and Unemancipated Minors. The Privacy Rule defers to State or other applicable laws that address the ability of a parent, guardian, or other person acting *in loco parentis* (collectively, “parent”) to obtain health information about a minor child. In most cases under the Rule, the parent is the personal representative of the minor child and can exercise the minor’s rights with respect to protected health information, because the parent usually has the authority to make health care decisions about his or her minor child. Regardless of whether a parent is the personal representative, the Privacy Rule permits a covered entity to disclose to a parent, or provide the parent with access to, a minor child’s protected health information when and to the extent it is expressly permitted or required by State or other laws (including relevant case law). Likewise, the Privacy Rule prohibits a covered entity from disclosing a minor child’s protected health information to a parent, or providing a parent with access to, such information when and to the extent it is expressly prohibited under State or other laws (including relevant case law). Thus, State and other applicable law governs when such law explicitly requires, permits, or prohibits the disclosure of, or access to, the health information about a minor child.

The Privacy Rule specifies three circumstances in which the parent is not the “personal representative” with respect to certain health information about his or her minor child. These exceptions generally track the ability of certain minors to obtain specified health care without parental consent under State or other laws, or standards of professional practice. In these situations, the parent does not control the minor’s health care decisions, and thus under the Rule, does not control the protected health information related to that care. The three exceptional circumstances when a parent is not the minor’s personal representative are:

- **When State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service;**

Example: A State law provides an adolescent the right to obtain mental health treatment without the consent of his or her parent, and the adolescent consents to such treatment without the parent’s consent.

- **When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor;**

Example: A court may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or the court may make the decision(s) itself.

- **When a parent agrees to a confidential relationship between the minor and the physician.**

Example: A physician asks the parent of a 16-year-old if the physician can talk with the child confidentially about a medical condition and the parent agrees.

Even in these exceptional circumstances, where the parent is not the “personal representative” of the minor, the Privacy Rule defers to State or other laws that require, permit, or prohibit the covered entity to disclose to a parent, or provide the parent access to, a minor child’s protected health information. Further, in these situations, if State or other law is silent or unclear concerning parental access to the minor’s protected health information, a covered entity has discretion to provide or deny a parent with access to the minor’s health information, if doing so is consistent with State or other applicable law, and provided the decision is made by a licensed health care professional in the exercise of professional judgment.

Abuse, Neglect, and Endangerment Situations. When a physician or other covered entity reasonably believes that an individual, including an unemancipated minor, has been or may be subjected to domestic violence, abuse or neglect by the personal representative, or that treating a person as an individual’s personal representative could endanger the individual, the covered entity may choose not to treat that person as the individual’s personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the individual. For example, if a physician reasonably believes that disclosing information about an incompetent elderly individual to the individual’s personal representative would endanger that individual, the Privacy Rule permits the physician to decline to make such disclosure.