February 2003

Prepared By Ropes & Gray
For The Association of Community Living Agencies In Mental Health

HIPAA 101: A BRIEF INTRODUCTION

PURPOSE

The purpose of this notice is to provide all health care professionals and residential program staff members with a brief introduction to new requirements concerning the protection of residents' privacy. The requirements were established by the federal law known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The United States Department of Health and Human Services has passed comprehensive privacy regulations that implement and enforce the requirements of HIPAA. These regulations went into effect on April 14, 2001 but will not be enforced by the government until the April 14, 2003 compliance date. These regulations do not simply replace existing federal and state laws that currently protect residential program residents' privacy, but will interact with these existing laws. Residential program policies will reflect this interaction and establish requirements for health care professionals and residential program staff. Please read this notice carefully and direct any questions to [insert contact person].

OVERVIEW OF THE HIPAA PRIVACY REGULATIONS

What activities are regulated by the HIPAA privacy regulations? The HIPAA privacy regulations are concerned with controlling the use and disclosure of a resident's health information where the information could potentially reveal the identity of the resident. This type of health information is referred to as "Protected Health Information" or "PHI." HIPAA regulates the use and disclosure of PHI by health care providers, health plans, and health care clearinghouses (which are entities that process or facilitate the processing of nonstandard data elements of health information into standard data elements, or vice versa). HIPAA generally prohibits health care providers, like our residential program, from using or disclosing PHI except as authorized by the residential program resident who is the subject of the information, or as permitted or required by the regulations. The privacy regulations, however, do not regulate or restrict the residential program's use or disclosure of health information that is "de-identified" so that it no longer has the potential to reveal the identity of the resident.

When can the residential program disclose PHI without first obtaining specific authorization from the resident? With the exception of certain types of information, the residential program may use and disclose PHI for treatment, payment and business operations if it has obtained a general written consent form from the resident that will cover these activities on an ongoing basis.[1] A specific authorization form is not required every time these activities are performed.

As a result, once a residential program has obtained the resident's general written consent, information may be shared between residential program staff members where necessary for those

individuals to provide treatment or care to the resident, obtain payment for the treatment or care and carry out business operations of the residential program. Information may also be shared with health care professionals for the same purposes if the health care professionals are part of an "organized health care arrangement" - which is discussed below.

In addition, the residential program may disclose PHI without a residential program resident's consent[2] or authorization to further certain public policy objectives, including:[3]

- Where disclosure is required by law;
- For a judicial or administrative proceeding;
- For public health activities;
- For health oversight activities;
- To report incidents of abuse, neglect or domestic violence;
- For law enforcement purposes;
- To avert a serious threat to health or safety;
- For national security and intelligence activities and protective services;
- For the health, safety or security of prison inmates or other detainees;
- To facilitate organ, eye or tissue donation; and
- To coroners, medical examiners, and funeral directors.

Certain types of information receive special protection. Under HIPAA, psychotherapy notes – which are notes by a mental health professional that document or analyze the contents of a counseling session and that are kept separate from the case record – are subject to heightened protection so that their use and disclosure generally requires specific authorization from the residential program resident. HIPAA also generally provides special protection to those types of information that have special protection under state law. New York provides special protection to mental health information, HIV-related information, alcohol and substance abuse treatment information and genetic information.

Under what circumstances can PHI be used for research purposes? PHI may be used or disclosed for research purposes only: (i) with resident authorization; (ii) after an IRB or privacy board approves the alteration or waiver of resident authorization; (iii) by/to a researcher for reviews preparatory to research; or (iv) by/to a researcher for research on the PHI of deceased persons.

Are there any limitations on the amount of PHI that can be used or disclosed? As a general rule, the residential program must take reasonable steps to limit the PHI that it uses and discloses, or that it requests from others, to the minimum amount that is necessary to accomplish the purpose of the use, disclosure, or request. This rule, however, does not apply when the residential program is disclosing or requesting PHI for treatment purposes, or when the residential program is using or disclosing PHI in a manner that is required by law.

To what extent can a residential program share PHI with health care professionals and facilities with whom it is clinically or operationally integrated? Legally separate health care providers that are clinically or operationally integrated may designate themselves as an "organized health care arrangement." For example, the residential program may be part of an organized health care arrangement with outside health care professionals who provide treatment or care to residents within the clinically integrated residential program setting. As members of an organized health care arrangement, residential program staff and health care professionals are permitted to share PHI for the health care operations of their joint enterprise, and may develop and use a joint notice of privacy practices covering all PHI created or received in connection with their joint enterprise.

What administrative requirements does HIPAA impose? The residential program must adopt policies and procedures to implement certain administrative requirements designed to protect the privacy of PHI, including:

- Designation of a privacy officer, who will in turn oversee the development, implementation and enforcement of the residential program's privacy policies and procedures;
- Employee training about the residential program's privacy policies and procedures; and
- Sanctions for employees who fail to follow the residential program's privacy policies and procedures.

The privacy regulations also require that the residential program limit its employees' access to PHI. Specifically, the residential program may permit access to PHI only by those employees with a "need to know" this information. Moreover, the residential program should, to the extent feasible, permit such employees to access only the information that is relevant to their job responsibilities.

What privacy rights do residents have under HIPAA? The privacy regulations grant residential program residents the following rights regarding their PHI:

- The right to notice of the residential program's privacy practices for PHI.
    - This notice must (i) generally explain the purposes for which the residential program may use and disclose the resident's PHI, (ii) inform the resident of his or her rights with respect to his or her PHI, and (iii) explain the residential program's legal duties under HIPAA. Our residential program must make a good faith effort to obtain a resident's written acknowledgement that he or she has received this notice of privacy practices.[4]
- The right to inspect and obtain a copy of their PHI.
- The right to request amendment or correction of their PHI.

- The right to receive an accounting list that provides information about disclosures of their PHI that were made to third parties for purposes other than treatment, payment and health care operations.

- The right to request that the residential program further restrict the way it uses or discloses their PHI.

- The right to request that the residential program communicate with them or with their personal representatives by alternative means or at alternative locations. The residential program must accommodate all reasonable requests.

To what extent can the residential program share PHI with third party vendors and other "business associates"? If a person or organization will create or receive PHI in order to perform an activity, function or service for the residential program, that entity will be considered a "business associate" of the residential program. Examples of business associates include billing services companies and transcription companies. Under the HIPAA privacy regulations, the residential program is required to enter into a contract with each business associate. The contract must include certain specific provisions to ensure that the business associate limits its uses and disclosures, and adequately safeguards the privacy, of the PHI that it receives from, or creates for, the residential program.

To what extent can the residential program share PHI with other health care providers? The residential program can generally share PHI with other health care providers where the residential program has obtained a general written consent[5] from the resident and the information is being shared so that the residential program or other health care provider can provide treatment to the resident or collect payment for that treatment. The residential program may also share PHI with other health care providers for certain health care operations (such as quality assurance, utilization review, or accreditation) as long as the recipient health care provider is required to comply with the HIPAA privacy regulations and the information relates to a relationship the provider has or had with the resident.[6]

What penalties may be imposed if the residential program fails to comply with HIPAA? HIPAA provides civil penalties for a failure to comply with the privacy regulations. The United States Department of Health and Human Services may impose civil monetary penalties of up to $100 for each violation (capped at $25,000 per person/entity per year for each standard violated). In addition, HIPAA provides for criminal penalties for intentionally obtaining or disclosing PHI in violation of the privacy regulations. Criminal sanctions may be imposed up to $250,000 and 10 years in prison.