

ATTACHMENT I
9 CSR 10-5.220 Privacy Rule of Health Insurance Portability and Accountability Act of 1996 (HIPAA)

PURPOSE: This rule alerts providers to the possible HIPAA Privacy Rule requirements if the provider has determined that it is a covered entity as defined by HIPAA. Once that is established, this rule lists policies and procedures that the HIPAA Privacy Rule requires for each covered entity.

(1) This rule applies to all programs licensed, certified or funded by the Department of Mental Health.

(2) Definitions.

(A) HIPAA: the Health Insurance Portability and Accountability Act of 1996 (45 CFR parts 160 and 164) as it relates to Privacy.

(B) Protected Health Information (PHI): As defined by HIPAA (45 CFR section 164.501), PHI is individually identifiable health information that is—

1. Transmitted by electronic media;
2. Maintained in any medium described in the definition of electronic media; or
3. Transmitted or maintained in any other form or medium.

(C) Individually identifiable health information: As defined by HIPAA (45 CFR section 160.103), individually identifiable health information is any information, including demographic information, collected from an individual that is—

1. Created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and
2. Related to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual, and which identifies the individual, or with respect to which there is reasonable basis to believe that the information can be used to identify the individual.

(D) Business associate: As defined by HIPAA (45 CFR section 160.103), a person who, on behalf of the covered entity or provider or of an organized healthcare arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

1. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
2. Any other function or activity regulated by this subchapter; or provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(3) All providers who determine that they qualify as covered entities must comply with the provisions of the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). A covered entity is defined as a healthcare provider, who transmits any health information in electronic form in connection with a transaction covered by this subchapter (section 160.103 of 45 CFR part 160), a health plan or a clearinghouse. The effective date of the Privacy Rule is April 14, 2003. IF this provider is a covered entity, THEN HIPAA requires the appropriate policies and procedures be in place to comply with the HIPAA Privacy Rule. HIPAA requires such policies and procedures to include, but not be limited to, the following topics: Notice of Privacy Practices, Amendment of Protected Health Information (PHI), Client Access to PHI, Accounting of Disclosures, Workforce Training, Verification, Authorization for Disclosures of PHI, HIPAA Complaint Process, Marketing (if applicable), Research (if applicable), Audit and Monitoring of HIPAA compliance, and Business Associates Agreements with those companies providing goods and services which require the disclosure of PHI, etc. Where existing confidentiality protections provided by 42 CFR part 2, related to the release of alcohol and drug abuse records, are greater than HIPAA, then the department anticipates that the provider will consider any such provision of 42 CFR part 2 as the guiding law.