Mental Health Information and the Electronic Medical Record: Risks and Solutions Specific to New York Providers

Increasingly, health care providers are replacing their paper-based records with a unified, comprehensive and provider-wide electronic medical record system. A significant advantage of switching from a paper to an electronic record is that electronic records provide medical practitioners with immediate access to the full medical histories of their patients as compiled by the many caregivers at the facility. As a general rule, as long as the electronic record system is compliant with the HIPAA security regulations, and protected health information is accessed, used and disclosed only for legitimate treatment, payment or health care operations purposes, or as otherwise permitted by the HIPAA privacy regulations, providers will be able to store and retrieve a full range of electronic records without violating patient privacy protections.

An exception to the general rule exists for hospital providers who operate a ward or unit that is licensed by the New York State Office of Mental Health ("OMH") or the New York State Office of Mental Retardation and Developmental Disabilities ("OMRDD"). Section 33.13 of New York's Mental Hygiene Law imposes on these licensed mental health providers privacy directives that are more stringent than, and thus not preempted by, HIPAA. One of the goals of HIPAA was to establish uniform national standards for protecting privacy. HIPAA did so by preempting all state laws whose protections were "contrary" to those afforded by HIPAA. Only state laws whose protections were "more stringent" than those imposed by HIPAA survived preemption. Because these "more stringent" laws were not preempted, they are still good laws, and must be complied with in addition to HIPAA. One of the protections afforded by Section 33.13 of the Mental Hygiene Law which survived preemption on the basis of being "more stringent" than HIPAA is its general prohibition against disclosing mental health information outside an OMH /OMRDD-licensed ward or unit. While there are some exceptions in Section 33.13 to this general prohibition,[1] there is no "treatment, payment and/or health care operations" exception that permits the disclosure of mental health information from the OMH/OMRDD-licensed ward or unit to other departments or units within the same hospital.

Thus, while HIPAA would not preclude a practitioner from within the covered entity, but outside the OMH/OMRDD-licensed ward or unit, from accessing mental health information maintained by that ward or unit for "treatment, payment and/or health care operations" purposes, such access is prohibited by Section 33.13. That the information is meant to stay within the ward or unit is underscored by the statutory definitions of "facility" and "provider of services,"[2] both of which specifically *exclude* any part of a general hospital not licensed by or operated by OMH or OMRDD. In short, the Mental Hygiene Law permits the free exchange of information within the mental health facility or OMH/OMRDD-

[1] The exceptions in Section 33.13 allow disclosure of mental hygiene records: (1) to a commission on quality of care; (2) with the consent of the patient, to persons and entities who have a demonstrable need for the information; (3) to governmental agencies or insurance companies for billing purposes, with consent of the commissioner; (4) to appropriate individuals or entities when necessary to prevent imminent serious harm; and (5) to qualified researchers upon approval of an institutional review board, with consent of the commissioner.

[2] "Provider of services" is defined as "an individual, association, corporation, or public or private agency, other than an agency or department of the state, which provides services for the mentally disabled. It shall not include any part of a hospital as defined in [Article 28] of the public health law which is not being operated for the purpose of providing services for the mentally disabled." N.Y. Mental Hyg. Law § 1.03(5).

licensed unit, but does not contemplate a regular exchange of information between the mental health unit of a hospital and the other areas of a general hospital in which the mental health unit is housed.

For those health care providers who wish to have a more integrated electronic medical record, certain steps can be taken to comply with the requirements of Section 33.13. One possible step would be to craft a patient consent form -- and to use the form routinely with mental health unit patients -- authorizing the inclusion of OMH/OMRDD-licensed mental health information within the electronic medical record itself, thus allowing all providers within all the units or clinics of one institution to access and use mental health information for standard treatment, payment and operations purposes related to that patient. Another somewhat less aggressive measure would be to seek routine patient consent to allow the inclusion of the protected mental hygiene information onto a segregated file of the unified electronic medical record and notifying patients in that consent form that their mental health information will only be accessible by practitioners as permitted by the provider's policies and procedures governing the electronic record and as otherwise permitted by Section 33.13. Although Section 33.13 does not mandate the content or form of a patient consent for these purposes, the most prudent approach would be to assure that the consent itself is unambiguous with respect to the patient's consent for institutional access and use of protected mental health information. A consent for these purposes could either be integrated into a standard admission consent or could be offered in a separate document at time of admission. In offering such separate consents to patients, however, hospitals and clinics should be be prepared to deal with the occasional patient who refuses such consent and whose mental health unit records therefore must be segregated.

If an institution wishes to include protected mental health information within a unified electronic medical record but does not find it feasible or necessary to seek routine patient consent for integration of the mental health information within the larger medical record, an alternative would be simply to "password-protect" the segregated mental health information file of the unified medical record system. In such a system, a patient's mental health information would be accessible only to authorized individuals, as defined in the electronic records policy, who are given the special mental health unit password. A weaker alternative to strict password protection would be for an electronic medical record to be configured at least to segregate the protected mental health information in a special file, and for a "pop-up" screen to arise whenever a staff member clicks on the mental health information icon, as a reminder that only authorized individuals may access that part of the electronic record. This last alternative, however, relies entirely on staff compliance with a policy against routine access to that portion of a medical record.

Because the Mental Hygiene Law requires a notation to be made whenever OMH/OMRDD-licensed mental health records are accessed by persons outside of the licensed mental health unit or program, the electronic record should be configured to generate an electronic notation of the user name, date and time whenever the protected mental health record is accessed. It would be good practice to design a system so that it encourages or requires a brief description of the scope or type of mental health information accessed, as well as the purpose for the disclosure. Regardless of the chosen safeguard(s), if OMH/OMRDD-licensed mental health records are incorporated into the unified electronic medical record, an audit system to monitor compliance with policies and procedures should be implemented, along with strict sanctions for non-compliance.

Please note that there are issues relating to inclusion of HIV, genetic testing, and substance abuse and alcoholism treatment information in a unified electronic medical record system, and these should also be carefully considered in designing a unified electronic medical record system.

Contact Information

Ropes & Gray continues to offer advanced privacy and HIPAA counseling to health care providers, and has worked extensively with clients who have developed a unified electronic medical record. If you have questions about this or related issues, please contact your regular contact at Ropes & Gray.