

Legal Brief

Medical Record Privacy – Covered Entities

This Legal Brief was drafted for general informational purposes only. It is not meant to be a comprehensive guide, nor should it be construed as legal advice. The information in this brief is current as of February 1, 2013; readers should consult the most recent versions of referenced statutes, regulations, and cases to ensure there have been no material changes.

Summary

The HIPAA mandated federal privacy rules apply to so-called “covered entities.” “Covered entities” are health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically. Covered entities may contract with others to carry out their obligations as covered entities.

Discussion

Under the Health Insurance Portability and Accountability Act of 1996 (herein “HIPAA”) mandated privacy rules, a covered entity may not use or disclose protected health information, except as permitted or required by the rules. Covered entities are broadly defined in the rules as health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically. “Transactions” is defined to include health care claims or equivalent encounter information, health care payment and remittance advice, coordination of benefits, health care claim status, enrollment and disenrollment in a health plan, eligibility for a health plan, health plan premium payments, referral certification and authorization, first report of injury, health claims attachments, and any other transaction that the Secretary of the Department of Health and Human Services may prescribe. 45 CFR §160.103. As a result of this broad definition, nearly all medical providers are subject to the HIPAA privacy rules.

Covered entities remain bound by the HIPPA privacy rules even if they contract with others - labeled by the regulations as “business associates” - to perform some of their essential functions. 45 CFR §146.502. When a covered entity contracts with a “business associate,” the covered entity and the business associate must enter into a contract addressing the party’s obligations vis-à-vis protected health information. 45 CFR §164.502(e). Although covered entities remain bound by HIPPA privacy rules, they are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. Nor is the covered entity responsible or liable for the actions of its business associates.

However, if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible, the covered entity must report the problem to the Department of Health and Human Services’ Office for Civil Rights. See 45 CFR §164.504(e)(1).

Conclusion

Covered entities are subject to the HIPAA mandated federal privacy rules. Covered entities that contract with others to carry out their obligations under the HIPAA privacy rules must enter into a contract to specifically protect health information. If the covered entity becomes aware of violations by its business associates, the covered entity must take remedial action.

Cross-References

Medical Record Privacy – Disclosure with Patient Consent

Medical Record Privacy – Patient Right of Access to Medical Records

Medical Record Privacy – Protected Health Information



SDSMA gratefully acknowledges the SDSMA Foundation for its support of this publication through funds awarded by The Physicians Foundation.