Health Information & the Law
HealthInfoLaw.org
Fast Facts November 2013

What activities are "healthcare operations" under the HIPAA Privacy Rule?

The HIPAA Privacy Rule sets a federal floor for the protection of personal health information and generally prohibits covered entities from using or disclosing protected health information (PHI) without the consent of the patient. However, to allow for the efficient operation of the system as a whole, the Privacy Rule permits covered entities to use and disclose PHI without patient consent for certain core activities: treatment, payment and healthcare operations. While treatment and payment are fairly self-explanatory, "healthcare operations" can be ambiguous.

To support the core functions of treatment and payment, a covered entity must engage in business practices that are necessary to run its business, such as certain legal, administrative, financial, and quality-related activities. These activities are collectively known as "healthcare operations" and do not require patient consent to use PHI to conduct them. The Privacy Rule lists (at 45 C.F.R. § 164.501) the specific activities that will qualify as operations:

- Conducting quality assessment and improvement activities;
- Population-based activities relating to improving health or reducing health care costs;
- Case management and care coordination;
- Reviewing the competence or qualifications of health care professionals;
- Evaluating provider and health plan performance;
- Training health care and non-health care professionals;
- Accreditation, certification, licensing, or credentialing activities;
- Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
- Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
- Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

While patient consent is not required, covered entities using and disclosing PHI for healthcare operations must only use and disclose the minimum amount of information necessary to accomplish the purpose of disclosure. An individual has the right to request limits on the use and disclosure of PHI for healthcare operations, but the covered entity is not required to agree. Finally, a covered entity must provide the patient with a notice of its privacy practices, and all uses and disclosures of PHI for healthcare operations without consent must be consistent with those practices.

For more information on state and federal laws related to privacy, see www.healthinfolaw.org/topics/63. For more information about HIPAA, see www.healthinfolaw.org/federal-law/HIPAA. Follow us on Twitter at **@HealthInfoLaw**