Business Associate HIPAA Compliance

February 18, 2013

The recent Omnibus HIPAA Regulations finalized changes under the HITECH Act to apply privacy and security requirements to Business Associates. Understanding the full impact of these regulations on businesses that contract with healthcare providers, health plans, and healthcare clearing houses ("Covered Entities") begins with an examination of the expanded definition of Business Associate under the law.

A Business Associate is a person not in a Covered Entity's workforce who, on behalf of the Covered Entity, assists in the performance of 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; repricing; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services; or any other function or activity regulated by HIPAA.

Under the new regulations, Business Associates are now responsible for HIPAA compliance and the Office of Civil Rights ("OCR") can enforce requirements and level HIPAA penalties directly against Business Associates. Business Associates may be held responsible for the actions or omissions of their own workforce and, in some situations, subcontractors with whom they share protected health information. To comply with the new regulations and protect the interests of Business Associates, Business Associates must now enter into written agreements with Subcontractors that comply with Business Associate Agreement requirements if the Subcontractor is permitted to use or access protected health information.

Of greatest significance to Business Associates is the requirement to implement administrative, physical, and technical safeguards to comply with the HIPAA Security Regulations as if they were Covered Entities. This requirement alone comprises half of the estimated $225.4 million in costs for Business Associates and Covered Entities to implement the new regulations. Compliance with this requirement involves more than just encryption of e-mails. Some of the more significant components of HIPAA Security compliance include:

- Identification and segregation of protected health information within information technology systems;
- Limitation of workforce access to protected health information to the amount necessary to perform job duties, including tracking and auditing of such access;
- Implementation of policies and procedures, staff education, and corrective action process;

- Performance of a security risk assessment and implementation of appropriate physical, technical, and administrative safeguards to appropriately manage identified risks;
- Development of a system to manage data back-up, disaster recovery, and emergency mode operations;
- Implementation of a system to monitor security of information systems containing electronic protected health information including review of audit logs and monitoring of staff compliance; and
- Identification and security of all media and devices containing electronic protected health information, including use of appropriate encryption, tracking of movement, and monitoring of use.

Covered Entities and Business Associates have until September 23, 2013 to implement the changes required to comply with these new requirements. If you have any questions about how these privacy and security requirements affect your company, please contact your Lathrop Gage attorney or any of the attorneys listed above.