HARRANG LONG GARY RUDNICK P.C.
ATTORNEYS & COUNSELORS AT LAW

October 9, 2009

NEW HEALTH SECURITY BREACH NOTIFICATION RULES

Interim final rules implementing security breach notification requirements for personal health data released by the Department of Health and Human Services (HHS) create new compliance obligations. The new HHS rule became effective on September 23, 2009.

The HHS breach notification rule governs security breaches involving information maintained by HIPAA-covered entities or business associates of HIPAA-covered entities. Business associates, in particular, will want to familiarize themselves with the new requirements. The HHS rule requires notification in the event of a breach involving *unsecured* data. The rule requires notice to affected individuals within 60 calendar days following discovery of the breach and, in the event that more than 500 individuals are affected, notice to the media.

Many entities that use or maintain personal health information have longstanding security measures in place in order to comply with the HIPAA security rule. However, data that is secured in accordance with the HIPAA security rule still may be breached in a manner that would trigger the notification obligations required under the new rule. To the extent that the HIPAA security rule and the HIPAA breach notification rule have some overlap, organizations subject to each will need to undertake an individual analysis to ensure they comply with both.

The new rules suggest the ongoing importance of monitoring legal and regulatory developments in this area to help ensure that compliance and risk-management procedures are current and can be implemented in a timely manner. The rules, coupled with continuing increased privacy regulations, emphasize the value of creating written incident-response policies to help coordinate responses. HHS guidance and commentary make clear the value to all healthcare businesses in planning for these issues as part of their compliance programs.

It appears likely that all organizations that use health-related data can expect increased emphasis on privacy and data protection in their contracts and should be prepared accordingly. As a practical matter, coupled with other recent changes to HIPAA, many organizations, especially business associates, may choose to review their existing policies and compliance programs as well as their risk management strategies for handling health-related data.

Harrang Long Gary Rudnick P.C.

For further information, please contact:

John A. Riherd
(541) 485-0220 (Eugene)
(503) 242-0000 (Portland)
john.riherd@harrang.com

Arden J. Olson
(541) 485-0220 (Eugene)
(503) 242-0000 (Portland)
arden.j.olson@harrang.com