# Health Information Compliance Alert

## BYOD Breach: Analyze 4 New Assessment Points

**Understand the new definition of 'breach of unsecured PHI.'**

If you have a breach of protected health information (PHI) — regardless of whether it's related to a "bring your own device" (BYOD) problem — you now have a new process for determining whether the breach posed a significant risk.

The **U.S. Department of Health and Human Services** issued the new final Omnibus Rule and published it in the Jan. 25 Federal Register. The rule implements a new definition of "breach," which now encompasses "any impermissible use or disclosure of PHI."

"Specifically, there is a new presumption that an unauthorized use or disclosure of unsecured PHI constitutes a breach unless the covered entity or business associate demonstrates a low probability that the PHI has been compromised," according to the law firm **Epstein Becker Green**. "Thus, entities will no longer be able to conduct analyses to determine whether uses or disclosures of PHI pose a significant risk of harm to individuals.

Instead, the Omnibus Rule mandates that you analyze the following:

1. The nature and extent of PHI involved in the use or disclosure, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized entity to whom the PHI was disclosed or who used the PHI;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

**Resource:** To view the entire Final Rule, go to www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.