On January 17, 2013, nearly 3 years after its initial proposed rule, the US Department of Health and Human Services (HHS) issued the long-awaited and much-anticipated Health Insurance Portability and Accountability Act (HIPAA) “omnibus” rule, extending the scope of the privacy law beyond healthcare providers to their business associates and subcontractors, and adding increased penalties for noncompliance.1

Regulated entities must be in compliance with the new rules by September 22, 2013, although covered entities and business associates will have up to 1 year after the 180-day compliance date to modify existing contracts to comply with these revised rules. All provider practices and health plans should begin to examine their policies now to ensure a seamless transition to these new rules.

All provider practices and health plans are now tasked with the arduous effort of implementing what the HHS is calling “the most sweeping changes to the HIPAA privacy and security rules since they were first implemented.”

Among the most dramatic changes to the existing law is that HIPAA’s privacy and security requirements will now directly apply to business associates.

Business associates will now include health information organizations, e-prescribing gateways, other entities that provide data transmission services for covered entities and that require access to data on a routine basis, entities that offer a personal health record to individuals on behalf of a covered entity, and subcontractors.

Penalties for noncompliance will range in severity, depending on the degree of culpability, including the number of individuals affected, and whether the noncompliant body has a history of noncompliance.

Central to the new regulations—which total a whopping 563 pages—is the sharing of patient-protected health information. Patients are given new control over their patient-protected health information, including allowing patients to request a copy of their electronic medical record in an electronic format and permitting patients to instruct their provider not to share information about treatment with their health plan when the individual pays for that care out of pocket.

In addition, the final rule expands the definition of a “breach” under HIPAA, thus eliminating the “harm” standard, which previously allowed entities to avoid breach notification if they could demonstrate that the breach posed no significant risk of harm to the individual. Under the new rule, any impermissible use or disclosure of patient-protected health information is presumed a breach, “regardless of whether the information is being held by a health plan, a healthcare provider, or one of their business associates,”1 unless a low probability that information has been compromised can be demonstrated.

All provider practices and health plans are now tasked with the arduous effort of implementing what the HHS is calling “the most sweeping changes to the HIPAA privacy and security rules since they were first implemented.”1

Reference