New HIPAA Final Regulations Amending Breach Definition & Civil Monetary Penalties

The HITECH Act requires Covered Entities to notify affected individuals of any breach of unsecured protected health information. The HITECH Act defined "breach" as the "unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information," subject to certain exceptions for unintentional or inadvertent disclosures. Then, in an interim final rule, which was effective Sept. 23, 2009, HHS defined "compromises the security or privacy of the protected health information" to mean "poses a significant risk of financial, reputational or other harm to the individual." Effective September 23, 2013, the new HIPAA regulations have changed the definition of breach to no longer include the "significant risk of harm" standard. The existence of a breach now depends on whether there is a "low probability" that the protected health information has been "compromised" based on the following four factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the protected health information or to whom the disclosure was made.
- Whether the protected health information was actually acquired or viewed.
- The extent to which the risk to the protected health information has been mitigated.

Under the new regulations, any acquisition, access, use or disclosure of protected health information not permitted by the Privacy Rule is presumed to be a breach unless the Covered Entity or Business Associate demonstrates the low probability of compromise by performing a risk assessment utilizing at least the four factors stated above. While the new regulations do not explain what it means for information to be "compromised," the new definition appears to remove much of the discretion a Covered Entity may have had under the prior definition in determining the existence of a breach based on a significant risk of harm. Additionally, it is now clear that the Covered Entity or Business Associate bears the burden of demonstrating that the information is not "compromised" in order to avoid determining that a breach has occurred. Practically, this does not appear to affect the result of a breach analysis in most cases. The primary exception is that if the recipient of information in a potential breach is unknown, then it appears impossible to demonstrate a low probability of compromise, whereas under the former rule a Covered Entity may have been able to find no substantial risk of harm to the affected individuals in some cases. Considering this new definition, all Covered Entities and Business Associates should consider encrypting any protected health information stored on mobile devices, such as laptops, tablets, and cell phones, so that if the device is lost or stolen, there will be a low risk of compromise and thereby limit this potential source of a breach. The new regulations also raise the liability for HIPAA violations to $100-$50,000 per violation with a $1.5 million annual cap and clarify the method by which HHS will calculate the penalties for such violations. Furthermore, the new regulations significantly expand liability by subjecting Business Associates and their downstream subcontractors to direct liability for certain HIPAA violations. The new regulations allow HHS to treat an ongoing violation of a provision or a violation affecting multiple individuals as multiple violations. Under the prior regulations, it was uncertain how HHS would apply a violation of a single provision that affected multiple individuals or continued over time without being cured. The new regulations provide that HHS will apply the number of violations of a single Privacy Rule provision deriving from a breach based on the number of individuals whose information was

disclosed. HHS could then render a fine up to $50,000 for each disclosure, multiplied by the number of individuals affected, subject to a cap of $1.5 million. Furthermore, the same breach could be the result of a separate violation for failure to implement adequate physical security of protected health information that is continued over a period of time. In that instance, the regulations permit HHS to count the number of times the provision was violated based on the number of days the violation continued. Based on the culpability level of the individual or entity, HHS could therefore impose a separate $50,000 fine for each violation of the Security Rule, multiplied by the number of days the violation occurred, subject to a separate cap of $1.5 million for the calendar year. Thus, in the above example, the individual or entity could face up to $3 million in potential liability.