HHS Fact Sheet Provides Helpful Information in Addressing Ransomware Attacks under HIPAA

August 25, 2016

The U.S. Department of Health and Human Services (?ÃÂ£***HHS***?ÃÂ¥) recently issued a ?ÃÂ£Fact Sheet?ÃÂ¥ which discusses ransomware attack prevention and recovery under HIPAA, as well as the management of HIPAA breach notification procedures in response to a ransomware attack. ?Ã¡According to the Fact Sheet, ?ÃÂ£ransomware?ÃÂ¥ is a type of malicious software by which a hacker gains access to electronic data and then encrypts it with a key known only to the hacker, such that the data owner is denied access to it. The Fact Sheet provides helpful descriptions and specific examples of how the requirements of the security regulations under HIPAA (the ?ÃÂ£***Security Rules***?ÃÂ¥), which govern the confidentiality of a HIPAA covered entity?ÃÃs electronic protected health information (?ÃÂ£***EPHI***?ÃÂ¥), may be applied to prevent, detect, and recover from infections of EPHI by ransomware. ?Ã¡Importantly, the Fact Sheet also explains HHS?ÃÃs view that a ransomware infection of unsecured EPHI on a computer system that is maintained for a covered entity, such as an employer-provided group health plan, is generally considered to be a ?ÃÂ£breach?ÃÂ¥ under the Security Rules. ?Ã¡This is because the EPHI encrypted by the ransomware was acquired (*i.e.*, taken control of) by an unauthorized individual, and thus an impermissible disclosure under HIPAA has occurred. The Fact Sheet reports there have been 4,000 daily ransomware attacks since early 2016 (a 300 percent increase over the number reported in 2015). In light of these sobering statistics, employers that sponsor group health plans that are covered entities under HIPAA would be well-advised to review the Fact Sheet and carefully consider this guidance when developing or maintaining compliance with the Security Rules. A copy of the Fact Sheet is available?Ã¡**here**.