

**Seyburn Kahn**  
**Health Law Update: April 1, 2014**

**Security Risk Assessment for Healthcare Organizations**

Numerous regulations have been issued under the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA Security Rule, issued on February 20, 2003, requires healthcare providers to conduct a security risk assessment. The Office for Civil Rights (OCR) and the National Coordinator for Health Information Technology (ONC), both within the Department of Health and Human Services, jointly issued a security risk assessment tool for healthcare providers.

Use of this security risk assessment tool is not mandated, but its free availability will make it difficult to justify not having conducted a risk assessment. The tool was made available on March 28, 2014, at [www.healthit.gov/providers-professionals/security-risk-assessment-tool](http://www.healthit.gov/providers-professionals/security-risk-assessment-tool). From this same webpage, users may also find a tip sheet related to the security risk assessment tool and other resources associated with compliance with the HIPAA Security Rule. The security risk assessment tool is available for both Windows and Apple operating systems, at no cost. Once a provider has worked through the self-security risk assessment tool, it will produce a report that the provider can furnish to an auditor inquiring into the provider's HIPAA Security Rule compliance preparedness.

The security risk assessment tool consists of 151 questions presented in an interview format. The user is responsible for identifying the materiality of each item. Although the security risk assessment tool will not challenge the user's chosen level of threat or vulnerability for any particular item as it applies to the user's business practices, an auditor reviewing the report generated by the security risk assessment tool may determine that the user did not fully appreciate the risk of an issue. The security risk assessment tool includes references to the HIPAA Security Rule as applicable to each question in the interview.

ONC was careful to state that the security risk assessment tool does not produce a statement of compliance with the HIPAA Security Rule. Instead, the security risk assessment tool is intended to help users identify missing or inadequate security controls as they relate to electronic protected health information.

† † †

Readers are welcome to direct questions to their regular Seyburn Kahn attorney or to Neal A. Cooper at [ncooper@seyburn.com](mailto:ncooper@seyburn.com) or 248-353-7620.