No More Excuses: HHS Issues New HIPAA Tool for Small Businesses

Three U.S. Department of Health and Human Services ("HHS") agencies, the Office for the National Coordinator for Health IT ("ONC"), in conjunction with the Office for Civil Rights ("OCR") and the Office of the General Counsel ("OGC"), have released a new security risk assessment ("SRA") tool to assist small to mid-sized organizations subject to the Health Insurance Portability and Accountability Act ("HIPAA") satisfy the security risk analysis obligations under the HIPAA Security Rule. While many covered entities and business associates may appropriately view the SRA tool as a new resource, some in the privacy and security community have raised concerns about the adequacy of the tool.

The HIPAA Security Rule requires covered entities and business associates to implement policies and procedures to prevent, detect, contain, and correct security violations, including conducting a security risk analysis, which is defined as an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by a covered entity or business associate. The SRA tool is intended to help covered entities and business associates meet this obligation by asking 156 detailed questions that focus on information security compliance risks. Users will find that the SRA tool presents a variety of questions about business practices and current security procedures, focusing on administrative, technical, and physical safeguards. The SRA tool organizes the responses entered in by the covered entity or business associate to provide guidance on what corrective actions may be needed, and to assist in developing targeted risk remediation plans.

The security risk analysis requirement under the HIPAA Security Rule has historically been a weak point in covered entity and business associate HIPAA compliance. The failure to conduct a security risk analysis has routinely been cited as a deficiency in OCR's compliance reviews and enforcement actions. For instance, in December 2013, a small Massachusetts-based dermatology practice experiences a reportable breach when a thumb drive with PHI was stolen from an employee's car. The dermatology practice, which employs only 12 physicians, notified all of its patients and the media about the data breach. Nonetheless, when OCR investigated the practice subsequent to the breach, OCR found that the practice had not conducted a thorough security risk analysis and included this violation in its calculation of the $150,000 fine the practice paid.

In addition to the potential HIPAA regulatory exposure, failure to conduct a security risk analysis may also jeopardize potential funds received under the Medicare and Medicaid Electronic Health Record ("EHR") Meaningful Use Incentive Program, which is administered by the Centers for Medicare and Medicaid Services ("CMS"), in conjunction with ONC and State Medicaid Agencies. Although primarily a program to support EHR adoption, the EHR Meaningful Use Incentive Program explicitly requires that eligible hospitals and eligible professionals attest that they have conducted a security risk analysis in compliance with HIPAA Security Rule in order to be eligible for incentives under the program each year. In conducting audits of those meaningful use attestations, CMS has recently found that eligible hospitals and eligible professionals are most commonly failing the audits due to failure to conduct a security risk analysis.

These enforcement actions and audit findings are especially worrisome for smaller covered entities and business associates with fewer resources to dedicate to the time-consuming and expensive task of analyzing and assessing data security. The new SRA tool is intended to assist small and mid-sized organizations with the burdens of compliance. While organizations may appropriately view the SRA tool as a new resource, they should also be aware that many in the privacy and security community have raised concerns about the tool. In particular, many have pointed out that "security risk assessment" is not in fact the correct terminology under the HIPAA Security Rule, given that the tool is targeted to ensuring compliance with the risk analysis

obligations rather than "assessment" obligations. In addition, the SRA tool does not closely follow much of HHS's prior guidance regarding how to fulfill the security risk analysis requirements under the HIPAA Security Rule. Lastly, the SRA tool contains several unhelpful disclaimers, including the fact that the tool is provided for information purposes only, that it does not serve as legal advice, and that is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks.

The application is available to download at www.HealthIT.gov/security-risk-assessment and from the Apple® App Store℠.

We will continue to monitor related HIPAA developments and the use of the SRA tool. If you have any questions with regard to the tool, or any other related matter, please contact Debbie Gersh, Tim McCrystal or your usual Ropes & Gray advisor.