PAUL HASTINGS
STAY CURRENT
A CLIENT ALERT FROM PAUL HASTINGS

April 2014

New HIPAA Tool Makes Compliance Easier, but may also Increase Likelihood of Enforcement

BY JAMES F. OWENS & JOSH R. HILL

Last month, the US Department of Health and Human Services (HHS) released a security risk assessment tool (SRA Tool) for use by covered entities, with the goal of increasing compliance with the HIPAA Security Rule by helping them perform proper risk assessments. While the tool is likely to help covered entities comply with the risk assessment obligations of HIPAA and thus result in less HIPAA violations, it may also increase enforcement against those who fail to satisfy risk assessment requirements, as the excuses for failure will be less persuasive now that the SRA Tool has been made available.

Risk Assessments and the SRA Tool

Under the HIPAA Security Rule, covered entities are required to perform risk assessments to evaluate organizational compliance with the Security Rule, identify areas susceptible to non-compliance and assess possible security threats to sensitive patient information, and establish policies and procedures for addressing suspect areas and fostering a culture of compliance. The SRA Tool, which is downloadable free of charge through HealthIT.gov, is intended to help guide covered entities through the risk assessment process and increase the likelihood of compliance. Nonetheless, while HHS considers the SRA Tool to be a useful instrument to help organizations that are challenged by risk assessment requirements, HHS also points out that use of the SRA Tool is not required and by no means guarantees compliance with HIPAA or applicable state privacy laws.

Reasons for Using the SRA Tool

Perhaps the most common feature of entities that have faced financial penalties from the government as a result of failing to comply with HIPAA is the lack of a satisfactory risk assessment. The failure to have proper risk assessment procedures in place not only prevents an organization from appropriately evaluating its own suspect areas and instances of non-compliance, but it also demonstrates a lack of effort, which is often viewed as deliberate noncompliance and thus draws increased scrutiny from federal regulators. For that reason, covered entities should take advantage of the SRA Tool, not only to improve their own risk assessment capabilities for purposes of decreasing the likelihood of HIPAA violations, but also to show that they are serious about the process and are putting forth good faith efforts to ensure compliance, as doing so is likely to weigh in an entity's favor when regulators evaluate different entities and exercise prosecutorial discretion. Additionally, establishing and following risk assessment procedures can be a very costly undertaking, and many small and mid-sized covered entities may have foregone such endeavors in the past simply to avoid the expense. The SRA Tool

should greatly reduce these costs, and thus prove to be a valuable resource for those entities that choose to take advantage of it.

Implications and Take Away

In the SRA Tool, HHS has provided covered entities with a valuable resource for satisfying risk assessment requirements of the HIPAA Security Rule, and all covered entities, but particularly small and mid-sized covered entities, should take advantage of it. Widespread use of the SRA Tool is likely to result in less instances of non-compliance with risk assessment obligations, and thus less financial penalties imposed against covered entities. However, while the SRA Tool is likely to benefit those entities who take advantage of it, it will also likely result in greater scrutiny and possibly increased penalties against those who still fail to satisfy risk assessment requirements, as such failures will be increasingly difficult to explain given the availability of the SRA Tool.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Atlanta

Phillip H. Street
1.404.815.2216
phillipstreet@paulhastings.com

W. Craig Smith
1.404.815.2366
craigsmith@paulhastings.com

Tara Ravi
1.404.815.2368
tararavi@paulhastings.com

Los Angeles

James F. Owens
1.213.683.6191
jamesowens@paulhastings.com

Paul A. Gomez
1.213.683.6132
paulgomez@paulhastings.com

Joshua R. Hill
1.213.683.6328
joshuahill@paulhastings.com

Jenny Wang
1.213.683.6119
jennywang@paulhastings.com

Tomer Konowiecki
1.213.683.6278
tomerkonowiecki@paulhastings.com