# HIPAA Breach by Express Scripts Vendor Triggers Plan Sponsor Actions

December 15, 2021

Many employers that sponsor a group health plan which is a "covered entity" subject to the HIPAA privacy and security rules have recently received notice from Express Scripts, Inc., a pharmacy benefit manager ("***ESI***"), regarding a cyberattack on the computer network of its subcontractor, Medical Review Institute of America ("***MRIA***"). This cyberattack apparently resulted in a HIPAA breach of current or former participants' protected health information ("***PHI***") under the plans. The breach notices were sent to the employers by ESI in its capacity as a HIPAA business associate of the plans.Â

A breach of unsecured PHI triggers notification obligations on the part of covered entities under HIPAA's breach notification regulations (the "***Breach Rules***"), including (i) notifications to the individuals whose PHI was involved in the breach (the "***Impacted Individuals***"), and (ii) notification to HHS. Such notifications are subject to specific requirements of the Breach Rules, including content and timing requirements.

ESI's breach notice to the plans indicated that MRIA has agreed to administer the notifications to the Impacted Individuals and provide them with credit monitoring services.Â

An employer that decides to accept MRIA's offer should consider the following:

- To ensure its own compliance obligations under the Breach Rules are met, the employer should obtain a copy of MRIA's draft notification to Impacted Individuals for legal review before it is issued by MRIA;
- The employer should confirm which party (*i.e.,* the employer, ESI, or MRIA) will be responsible for the HHS notification required by the Breach Rules;
- The employer should determine whether the breach triggered notification and/or other obligations under state privacy laws and, if so, which party will be responsible for meeting such obligations; and
- The employer should determine what rights it may have to indemnification (*e.g.*, under a HIPAA business associate agreement) from ESI or MRIA in the event of any noncompliance with the Breach Rules.

Alternatively, if an employer intends to administer the breach notifications itself, the employer will then need to ensure that each of the required notifications conform to the content, delivery, timing, and other requirements of the Breach Rules.