FAILURE TO PROPERLY ASSESS BREACH RISK RESULTS IN $2.175 MILLION FINE TO AFFILIATED COVERED ENTITY

On November 27, 2019, the Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") announced that an Affiliated Covered Entity made up of 10 hospital covered entities ("ACE Organization") will pay a penalty of $2.175 million and enter into a two-year Corrective Action Plan ("CAP") to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Breach Notification Rule and Privacy Rule.

REGULATORY BACKGROUND – ACE STATUS UNDER HIPAA

To fully understand the significance of the alleged violations, it is helpful to first understand what an affiliated covered entity is and why one is formed. HIPAA allows legally separate covered entities to designate themselves, in writing, as a single affiliated covered entity ("ACE") when all of the covered entities are under "common ownership" or "common control." "Common control" is established when one entity has significant power to influence or direct the actions or policies of the other entities. "Common ownership" is established if one entity possesses a five percent or more interest in the other entities.

Covered entities may choose to designate themselves an ACE because such status can ease data-sharing between covered entities and reduce the administrative and operational burden of HIPAA compliance. Sharing protected health information ("PHI") between covered entities within an ACE is considered a "use" within the ACE as a single covered entity, instead of a "disclosure" to an outside entity. ACE status also allows covered entities to streamline HIPAA compliance efforts under a singular program. This includes enabling the ACE member entities to use the same set of policies and procedures, designate a common privacy officer and security officer, issue a single Notice of Privacy Practices and use one standard training program for workforce members. Further, business associate agreements may be entered into directly with the ACE and will apply to all ACE members.

However, ACE members also subject themselves to joint and several liability for any violations of HIPAA. The parties can agree to allocate risk contractually to mitigate uncertainty, but resolving disputes can prove burdensome. If entities form an ACE, they need to make sure their operations reflect such status.

THE POTENTIAL VIOLATIONS

Breach Notification

A complaint was filed with HHS alleging that a bill with another patient's PHI was sent to an individual on April 17, 2017. OCR's investigation determined that billing statements for almost 600 patients were merged with over 16,000 guarantor mailing labels, resulting in the improper disclosure of those patients' PHI, including name, account numbers and dates of service. The ACE Organization had performed its own investigation and conducted a breach risk assessment related to the incident. However, per OCR, the ACE Organization wrongly concluded that only disclosures including patient diagnosis, treatment information or other medical information resulted in a reportable breach of PHI. Therefore, the ACE Organization only reported the breach as affecting eight individuals whose medical information was disclosed. Additionally, the ACE Organization persisted in refusing to properly report the breach even after OCR explicitly advised them of their duty. As part of the CAP, the ACE Organization is required to review, revise and regularly update their policies and procedures consistent with the Breach Notification Rule and obtain HHS's approval of such policies, distribute revised policies to its workforce and obtain signed compliance certificates from workforce members, and report to HHS any event that the ACE Organization has determined not to be a reportable breach along with its breach risk assessment.

Lack of Business Associate Agreement

Additionally, during its investigation, OCR determined that the parent corporation of the hospital covered entities participating in the ACE Organization ("Parent Entity") performed services for the member hospitals that involved the receipt, maintenance and disclosure of PHI. Therefore, the ACE Organization and the Parent Entity were required to enter into a business associate agreement. However, neither the ACE Organization nor its individual covered entity members entered into a business associate agreement with the Parent Entity until October 17, 2018.

PRACTICAL TAKEAWAYS

In light of this enforcement action, all covered entities and business associates, but particularly ACEs and their non-covered entity parent organizations, should take note of the following:

- When a parent company that is not a covered entity provides services such as centralized billing to its subsidiaries that are covered entities, such as centralized billing, the parent company must enter into a business associate agreement with its covered entity subsidiaries covering such services. If its covered entity subsidiaries have formed an ACE, that parent entity may enter into one business associate agreement with the ACE to satisfy this requirement. Note that as a non-covered entity, the parent company cannot be a member of the ACE.
- Every time a potential reportable breach is discovered, HIPAA requires that a risk assessment be performed to determine whether the breach is reportable, at a minimum, taking into account the four factors set forth in the Breach Notification Rule. Thorough analysis and documentation of every risk assessment should be maintained to support the covered entity's conclusion regarding whether or not the breach is reportable. Such documentation can be quite valuable in demonstrating to OCR that the Breach Notification Rule's requirements were followed in the event of an investigation.
- If a covered entity does not correctly analyze the breach when it performs its risk assessment, such that the breach is not reported when the regulations required it, the failure to report the breach will still be considered a violation of the Breach Notification Rule by OCR. This potentially means that if OCR disagrees with the result of a covered entity's breach risk assessment, it can find the covered entity to have violated the Breach Notification Rule despite the entity following the process set forth in the regulations. Therefore, it may be wise for covered entities to use caution whenever determining a breach to be non-reportable and ensure that no such determination is made without sufficient supporting documentation.
- When determining whether to form an ACE, remember that the violation of one member entity can subject all member entities to regulatory scrutiny, any negative consequences will likely apply to all member entities, and all member entities will be jointly and severally liable for any financial penalty or settlement.

If you have any questions or would like additional information about this topic, please contact:

- Stephane Fabus at (317) 977-1406 or sfabus@hallrender.com;
- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com; or
- Your regular Hall Render attorney.

For more information on Hall Render's HIPAA, Privacy & Security services, click here.