O'NEILCANNON
HOLLMAN DEJONG & LAING S.C.

EMPLOYMENT LAWSCENE ALERT: REMEMBER MARCH 1 DEADLINE FOR REPORTING A "SMALL" HIPAA BREACH

Employers who are classified as covered entities under HIPAA are required to report any 2018 breach of protected health information that affected fewer than 500 individuals (also known as a small breach) by March 1, 2019. This current breach notification requirement arises from amendments made to HIPAA under the Health Information Technology for Economic and Clinical Health (HITECH) Act, as finalized in 2013. HIPAA defines a covered entity as either (1) a group health plan, (2) a health care clearinghouse, or (3) a health care provider who electronically transmits any protected health information. A covered entity may be an individual, an institution, or an organization.

Background

Under applicable rules, a breach is defined as an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information. Some exceptions apply, so that not all incidents will rise to the level of a breach. Still, an impermissible use or disclosure of protected health information is generally presumed to be a breach unless the covered entity demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of several specified factors.

Notification Requirement

Upon the occurrence of a confirmed (or in some cases, suspected) breach, the affected individuals must be provided with detailed notification letters without unreasonable delay and no later than 60 days after the discovery of the breach. While the covered entity, most often, provides the required notifications, the final rules permit the delegation of reporting duties to a business associate.

A HIPAA breach also triggers an obligation to notify the Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS).

- When a breach affects 500 or more individuals, the reporting entity must notify OCR contemporaneously with the notification to individuals (and must also notify local media

outlets).
- Where a breach affects fewer than 500 individuals (also known as a small breach), however, a reporting entity must maintain a log or other documentation of all breaches occurring during the year, and annually report all such breaches no later than 60 days after the end of that calendar year.

For a small breach occurring any time in 2018, the deadline to report that breach to OCR is March 1, 2019.

Small Breach Reporting Details

A reporting entity is not required to wait until the March 1 deadline to report a small breach. Small breaches may be reported as early as contemporaneously with the occurrence of the breach. Regardless of timing, all small breaches must be reported to OCR in the same manner. Specifically a reporting entity must report the breaches online through the OCR's "Breach Portal."

Note that even when a covered entity delegates the reporting function to a business associate, the covered entity retains ultimate legal responsibility for proper reporting. Accordingly, covered entities who delegate reporting may want to require proof of timely reporting.

Be aware that, while the reporting entity may report all small breaches on a single date, each separate breach incident will require a separate submission. Instead of simply uploading a log of breach incidents occurring in the prior year, the reporting entity must complete a six-section questionnaire to provide: (1) general information; (2) identification of the covered entity, business associate, and relevant contact information; (3) the nature of the breach; (4) a summary of related notices provided and actions taken; (5) an attestation, and; (6) a summary. Multiple fields must be completed within each of these six sections. The HIPAA status of a reporting party (as either a HIPAA covered entity or a business associate) must be indicated on the "Contact" tab of the online filing form.

The online reporting form also requires the reporting entity to indicate the level of pre-breach HIPAA compliance status, including whether or not HIPAA Privacy Rule safeguards and HIPAA Security Rule safeguards were in place.

Because filing the breach notice can be time-consuming, parties tasked with reporting 2018 small HIPAA breaches of unsecured protected health information are advised to gather and prepare the content to be reported before actually logging on to the OCR Breach Portal. Because any changes or updates to the submitted information must be entered as a separate entry, it is preferable to ensure that each submission is fully accurate. Moreover, because the content of Breach Notifications to OCR can form the basis for a future OCR investigation and enforcement action, it is advisable to have legal counsel review content prior to submission.

In addition to ensuring that 2018 breaches affecting fewer than 500 individuals are reported by March 1, covered entities and business associates should continue to ensure that HIPAA Policies and Procedures, as well as the applicable administrative, physical and technical safeguards are up to date and periodically reviewed.