OCR Annual Report on HIPAA Compliance and Breaches of Health Information

3/30/2023

On February 17, 2023, the U.S. Department of Health & Human Services, Office for Civil Rights (OCR) published its Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2021. While a slight decrease from calendar year 2020, in calendar year 2021 the OCR received 609 notifications of breaches of "unsecured" protected health information (PHI) affecting 500 or more individuals. Although the number of notifications in this category was only 609, the number of individuals affected by such breach events was 37,182,558. Monetary penalties totaled $5,125,000.

The covered entities and business associates implicated in these breach events included:

•437 reports (72%) of breaches from health care providers (affecting 24,389,630 individuals (66%))

•93 reports (15%) of breaches from health plans (affecting 3,236,443 individuals (9%))

•77 reports (13%) of breaches from business associates (affecting 9,554,023 individuals (26%))

•2 reports (<1%) of breaches from health care clearinghouses (affecting 2,462 individuals (<1%))

The types of breach events included:

•Hacking/IT incident of electronic equipment or a network server (459 reports (75%) affecting 35,264,773 individuals (95%))

•Unauthorized access or disclosure of records containing PHI (115 reports (19%) affecting 1,569,765 individuals (4%))

•Theft of electronic equipment/portable devices or paper containing PHI (21 reports (3%) affecting 123,615 individuals (<1%))

•Loss of electronic media or paper records containing PHI (9 reports (1%) affecting 33,845 individuals (<1%))

•Improper disposal of PHI (5 reports (1%) affecting 190,540 individuals (1%))

As to hacking/IT incidents, OCR reported that the "largest breach in 2021 [resulted] from a hacking/IT incident in which two former employees hacked the server of a healthcare provider containing ePHI. The breach incident affected 3,253,822 individuals. Other hacking/IT incidents involved the use of malware, ransomware, phishing, and the posting of PHI to public websites."

With respect to reported breaches involving fewer than 500 individuals, OCR received 63,571 reports, affecting a total of 319,215 individuals. In order of frequency, these included unauthorized access or disclosure (65%), loss (3%), hacking/IT incidents (1%), theft (1%), and improper disposal (2%).

The OCR's report highlights the types of threats to PHI faced by the health care industry; the takeaway is that covered entities and business associates must be ever-vigilant in maintaining a strong privacy and security program, including periodic risks assessments to identify and address potential threats and vulnerabilities to PHI, whether paper or electronic.

Click here to read the entire March 2023 Healthcare Law Update

For assistance with your organization's privacy and security program, contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com