October 28, 2020

Aetna Pays $1,000,000 to Settle Three HIPAA Breaches

Aetna Life Insurance Company and the affiliated covered entity (Aetna) has agreed to pay $1,000,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to adopt a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. Aetna is an American managed health care company that sells traditional and consumer-directed health insurance and related services.

In June 2017, Aetna submitted a breach report to OCR stating that on April 27, 2017, Aetna discovered that two web services used to display plan-related documents to health plan members allowed documents to be accessible without login credentials and subsequently indexed by various internet search engines. Aetna reported that 5,002 individuals were affected by this breach, and the protected health information (PHI) disclosed included names, insurance identification numbers, claim payment amounts, procedures service codes, and dates of service.

In August 2017, Aetna submitted a breach report to OCR stating that on July 28, 2017, benefit notices were mailed to members using window envelopes. Shortly after the mailing, Aetna received complaints from members that the words "HIV medication" could be seen through the envelope's window below the member's name and address. Aetna reported that 11,887 individuals were affected by this impermissible disclosure.

In November 2017, Aetna submitted a breach report to OCR stating that on September 25, 2017, a research study mailing sent to Aetna plan members contained the name and logo of the atrial fibrillation (irregular heartbeat) research study in which they were participating, on the envelope. Aetna reported that 1,600 individuals were affected by this impermissible disclosure.

OCR's investigation revealed that in addition to the impermissible disclosures, Aetna failed to perform periodic technical and nontechnical evaluations of operational changes affecting the security of their electronic PHI (ePHI); implement procedures to verify the identity of persons or entities seeking access to ePHI; limit PHI disclosures to the minimum necessary to accomplish the purpose of the use or disclosure; and have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

"When individuals contract for health insurance, they expect plans to keep their medical information safe from public exposure. Unfortunately, Aetna's failure to follow the HIPAA Rules resulted in three breaches in a six-month period, leading to this million dollar settlement," said OCR Director Roger Severino.

In addition to the monetary settlement, Aetna will undertake a corrective action plan that includes two years of monitoring. The resolution agreement and corrective action plan may be found at: https://www.hhs.gov/sites/default/files/aetna-ra-cap.pdf.*

*People using assistive technology may not be able to fully access information in this file. For assistance, contact the HHS Office for Civil Rights at (800) 368-1019, TDD toll-free: (800) 537-7697, or by emailing OCRMail@hhs.gov.

###