DWT releases latest health care breach charts

Blog **Privacy & Security Law Blog**

USA | November 11 2015

Safeguarding patient information is at the core of responsibilities for health care entities under the Health Insurance Portability and Accountability Act (HIPAA). But safeguarding patient information isn't just a regulatory requirement; every medical professional who takes the Hippocratic Oath (Modern Version) swears to respect patient privacy. To help covered entities and business associates better understand the vulnerabilities and threats to patient information and trends in the health care sector, DWT has distilled the latest information concerning larger HIPAA breaches offered by the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) into a series of charts, provided here.

OCR provides data on its website for data breaches of unsecured protected health information affecting 500 or more individuals that are self-reported by (or on behalf of) covered entities to OCR. DWT has compiled charts synthesizing the most recent breach data from OCR. The first set of charts looks at all breaches reported to OCR, by the cause of breach and the type of media involved. We also provide charts by the number of breach incidents reported as well as by number of individuals affected, as this may help understand causes or types of media (paper, laptop, email, portable electronic device, etc.) that affect a disproportionate number of individuals. Other charts focus on breaches involving business associates. Finally, we include charts illustrating the number of breaches and number of individuals affected by type of entity involved (i.e., type of covered entity or business associate).

Given the number of large data breaches affecting health care entities in 2015, it is no surprise that the number of individuals affected by a breach in the health care sector has increased dramatically in the past year. Beyond the increase in the sheer volume of individuals affected by breaches, however, there have not been dramatic changes in the data released by OCR since 2014. Indeed, although the number of breaches reported to OCR involving 500 or more individuals increased from 985 in May 2014 to 1,305 incidents by September 2015, the root causes of the reported breaches shifted very little. For instance, in May of 2014, the number one cause of a breach was due to theft, which accounted for 48%,

while in September 2015, theft comprised 49% of all reported breaches. Similarly, unauthorized access or disclosure comprised 17% of reported breaches in May 2014; by September 2015, that figure only increased 3% to 20% of all reported breaches.

Security incidents affecting patient information still are a serious and costly concern for all health care entities, regardless of their size. According to the Ponemon Institute's *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data*, the average cost of a breach affecting a health care organization is $2.1 million, while business associates face an average cost of $1 million to respond to a breach. Meanwhile, half of the entities surveyed by the Ponemon Institute reported having little-to-no confidence in being able to detect all patient data loss or theft, and a majority of both health care organizations and business associates reported having inadequate funding and resources to devote to their incident response processes.

Davis Wright Tremaine LLP - Bryan Thompson and Anna C. Watterson