



Issued 2/22/17

400K Patient Records Lost in January Health Care Breaches

Insider threats dominated Protenus' Health Care Breach Barometer with just over half of the compromised patient records that were lost in January being the result of either malicious or unintentional action by an insider. Protenus reported there were 31 breach incidents involving health care facilities during the first month of 2017 reported to the federal Health and Human Services department or made public in another manner resulting in 388,307 patient records being exposed. This figure was far below the 1.4 million records compromised during December 2016.

Nine of the 31 breaches during January were the result of insider actions – with five being specific malicious actions conducted by a worker and the remaining four simple errors that led to data being compromised, the report stated. The nine breaches all together were responsible for 59.2 percent, or 230,044, of the records exposed during the month with the intentional actions being responsible for 226,798.

Twelve of the January incidents were the result of the health care institution being hacked. These resulted in 145,636 records being compromised. The hacks came in several different flavors.

One was an extortion attempt from TheDarkOverlord who leaked patient data when the organization refused to pay the ransom. Another attack was

not looking for a financial reward, but instead interfered with a facility's ability to access data for marijuana records and prescriptions.

Other occurrences took place when employees fell for phishing scams, which were not classified as insider error because an outside entity spurred the unintentional release of data.