Program Brokerage Corporation

Cyber Healthcare Claims

Ransomware:

A recent spate of ransomware attacks (in which malware encrypts a user's and/or network's data and only unlocks it upon payment of a ransom, often in the form of untraceable bitcoin) has crippled hospitals across the nation.

- Hollywood Presbyterian Medical Center in Malibu, California paid around 40 bitcoin (valued at $17,000) when malware held their data hostage for over a week during February 2016.
- MedStar Health in Washington, DC and Maryland, with 10 hospitals and over 250 outpatient care centers, was asked for $19,000 in bitcoin when its data was locked by sophisticated ransomware in March 2016.

The potential for significant harm is obvious, as some sources have alleged not only that patient care and safety was directly affected by the network outage, but also that patients were turned away from care centers.

Regulatory Fines & Penalties:

On the other side of the cyber claim spectrum for healthcare organizations, simple employee accident or theft of a portable device has recently resulted in hefty HIPAA fines and penalties imposed by the U.S. Department of Health and Human Services' Office for Civil Rights (OCR). Formal penalties issued recently by the OCR have hit both a HIPAA "business associate" and a university hospital.

- The non-profit Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) was penalized $650,000 for a breach affective only 412 individuals. CHCS was serving as a business associate, providing information technology services, for local skilled nursing facilities. In 2014, an employee's company cell phone was stolen, and although it's unknown whether the patient data was actually accessed, OCR noted that the phone was unencrypted and had no password protection, in addition to the fact that CHCS did not have an Incident Response Plan in place or policies governing mobile devices containing protected information.

- The University of Mississippi Medical Center agreed to settle with the OCR for $2.75 million over allegations that up to 10,000 patients' information may have been accessible via an unencrypted stolen laptop with weak security controls.

In both cases, OCR focused its criticism of the organizations on the lack of controls in place, and not the fact that the data may have been breached.