

CHICAGO, IL, September 24, 2013 **/24-7PressRelease/** -- Over 1,400 patients in the Chicago area are being notified after the University of Chicago's Physicians Group realized that their private information had been compromised. The information included the patient's name, health treatment information, insurance data, date of birth, address, diagnosis, and their social security numbers. [Sonia](#)

[Ben-Yehuda](#)

explains that this information is often used for identity theft.

The breach occurred after the university contracted with a debt collection agency, which unintentionally allowed the information to become accessible to users on the Internet. The debt collector, ICS Collection Service received a report on July 9th that users were able to access sensitive information regarding other debtors while using its website.

According to ICS representatives, the company immediately launched an internal investigation once they received a report about the [breach](#) . They also contacted their third-party website and software vendors in order to determine how the breach could have occurred. The website helped the company correct the security setting and quickly disabled user access to certain pages. Sonia Ben-Yehuda notes that if a user had not reported the breach, the data would still be available for misuse.

ICS explained that the website was used by debtors to make payments and other account adjustments. It's important to note that the University of Chicago Physicians Group (UCPG) had previously contracted with ICS but that the contract had been terminated prior to the breach. Despite the termination, ICS retained the data of over 1,300 patients whose claims were active when the agreement ended.

Although ICS can expect consequences for this misuse of information, UCPG might also be liable even though they were not under contract during the breach.

The Health Insurance Portability and Accountability Act (HIPAA), stipulates that subcontractors and business associates of HIPAA covered entities are equally responsible for any type of privacy or security breach when it concerns protected health information. According to Sonia Ben-Yehuda, the privacy rule is balanced so that it allows health information to be disclosed when it is needed for proper patient care.

Only 16 out of more than 80,000 privacy and security breach cases have resulted in hefty fines

Sonia Ben-Yehuda Dissects HIPAA Data Breach

Written by Australian Business

since 2003. The Office for Civil Rights notes that these breaches have increased over the last few years as more and more companies begin to improperly utilize websites to store information. Sonia Ben-Yehuda agrees that it is too early to tell how the Office for Civil Rights will handle this complicated breach.

According to the Office for Civil Rights, which enforces HIPAA, the department has collected over \$18 million in fines from HIPAA violations and settlements. In August, the office announced a settlement of \$1.2 million with the New York-based Affinity Health Plan after the company neglected to erase protected health information. In that case, Affinity failed to erase information for more than 344,000 patients that have been saved to leased photocopiers.

Sonia Ben-Yehuda notes that misuse of protected health information has become an increasingly important issue as hospitals struggle to find ways to safely store massive amounts of patient data. With more patients to care for, stakeholders to coordinate and a limited budget, it can be extremely important for healthcare companies to keep their information organized and protected, which is an absolute must.

ABOUT

[Sonia Ben-Yehuda](#) co-founded MedCPU, Inc in 2008 and now serves as its President. Sonia Ben-Yehuda is respected as an entrepreneur in the healthcare IT technology industry and has experience with patient data storing services.