Press Release

Unsecured medical records expose patients to potential identity fraud

CoreID Services president Daniel J. Benish available for comment on the human toll of identity theft.

April 30, 2012 – Atlanta, GA. *For immediate release.* Emory Healthcare has reported that information on approximately 315,000 surgical patients has been misplaced. The data, which included patients' names, birth dates, diagnoses and, in some cases, Social Security numbers, were stored on back-up disks in an unsecured location in violation of the hospital's security policy.

Dan Benish, president of CoreID Services, LLC, an identity theft recovery firm based in Atlanta, GA, knows only too well the potential risks to the patients involved in this data loss. "When you hear of incidents like these, the focus tends to be on the number of records lost, especially when the numbers reach into the hundreds of thousands like it has at Emory Healthcare." Indeed, the larger the exposure, the greater the costs are for the organization involved, particularly if they must provide identity recovery services to correct fraudulent use.

But Benish knows that the real toll is at the human level. "When a victim's identity is stolen, they are in the position of 'guilty until proven innocent.' The burden is upon them to prove that they did not perform the fraud, whether it was incurring credit card charges, filing an insurance claim, leasing an apartment, opening a bank account, and so on."

This is the situation Warren Brown has faced ever since he realized his personal identifying information (PII) was stolen in May 2008. Despite trying to rectify the situation for the past four years – an effort that has generated enough paperwork to fill a three-ring binder – Brown was notified by the IRS this month that a fraudulent tax return was filed in his name. This latest incident, a common form of identity theft that allows thieves to collect victims' tax refunds, prompted him to contact CoreID Services for help.

CoreID Services manages the identity recovery process on behalf of their clients. Says Benish, "Clearing up identity theft is like clearing up a bad rash. You have to be vigilant about completely eradicating it, or it can keep coming back. It is very difficult for an individual to perform and confirm every step necessary to clear their identity." Organizations that experience data losses, either through hacking attempts or human error (as is believed to be the case at Emory Healthcare), are required to offer recovery services like CoreID 's ARX-ID identity recovery plan in order to comply with the HITECH Act.

Medical records are a common target for identity thieves. A recent survey report, entitled the "2012 HIMSS Analytics Report: Security of Patient Data," reported that 27% of the 250 surveyed healthcare providers had experienced a data breach in the past 12 months, most commonly due to improper access of patient health information (PHI) by an employee.

In response to this growing problem, the HITECH Act extends the reach of the HIPAA patient privacy laws to encompass business associates such as electronic patient record software providers, and to impose penalties for improper PHI handling. The HITECH Act required Emory Healthcare to self-report the lost records, notify all affected patients, and to provide recovery services should fraud be detected.

Emory Healthcare is recommending patients included in the data loss to regularly review their credit activity and request free annual credit reports to help them uncover any identity theft.

To speak with Mr. Benish on recovering from identity theft or its impact on victims, please contact CoreID Services, LLC at 855-262-7610 or email dbenish@coreidservices.com.

# # # # #

About CoreID Services, LLC

CoreID Services, LLC provides the ARX-ID™ suite of identity protection and recovery services. Their fully-managed identity recovery service allows CoreID to act on identity victim's behalf to perform all necessary tasks to report and resolve identity theft. Additional services also allow individuals to monitor their identities against all known data sources and generate real-time actionable alerts to minimize the impact of identity theft. Call 855-262-7610 or visit www.coreidservices.com to learn more.

Contact:

Helen Lawson
SpotOn Marketing
hnlawson@comcast.net
404-295-5921

Daniel J. Benish
President
CoreID Services, LLC
dbenish@coreidservices.com
855-262-7610