eALERT

INCompliance

August 18, 2014

**Hospital System Discloses HIPAA Breach Affecting 4.5 Million Individuals**

In an August 18, 2014, regulatory filing, Community Health Systems (CHS) disclosed that a group of Chinese hackers obtained patient information on 4.5 million individuals by infiltrating its computer network. This is the second-largest HIPAA breach on record.

CHS is based in Tennessee and operates hospitals in 29 states. The report, filed with the Securities and Exchange Commission (SEC), states the hackers breached the CHS computer network's security in April and June 2014. CHS reported that the hackers used "highly sophisticated malware and technology" to bypass security measures and successfully copy and transfer data outside CHS.

The compromised data included names, addresses, birthdates, telephone numbers and social security numbers of individuals who, in the last five years, were referred for or received services from physicians affiliated with CHS. As this information constitutes protected health information under HIPAA, CHS has notified the affected individuals and the U.S. Department of Health and Human Services of the breach. CHS is offering identify theft protection to individuals whose information was breached.

CHS also reported that it has engaged a forensic expert to investigate the incident and to assist CHS with remediation efforts. The malware has been completely removed from all CHS systems, according to the report. CHS also stated that it has implemented new security measures designed to protect against future attacks.

HHS posts information regarding reported breaches of protected health information affecting 500 or more individuals to its website. The largest breach listed on the site affected 4.9 million individuals and was reported by TRICARE Management Activity in 2011. Including the CHS breach, there have been seven breaches affecting more than one million individuals since reporting began in 2009.

The CHS breach report highlights the critical importance of strong electronic security measures for all covered entities and business associates. After security measures are implemented, they should be tested and reevaluated on a regular basis in order to keep pace with hackers, whose methods are constantly evolving. The CHS report is available on the SEC website.

INCompliance HIPAA consultants combine legal training with practical experience in the health care and health insurance industries. Most have a decade or more of experience with HIPAA privacy and security requirements. This combination of experience and knowledge uniquely

qualifies us to provide substantive and practical advice to help health care organizations, health plans, and business associates remain compliant in a rapidly changing world. To learn about these services, including the HIPAA Compliance and Audit Program, click here.

*This E-Alert was prepared by Chris Bennington. Chris can be reached at 513.870.6572 or cbennington@incomplianceconsulting.com. Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com. This and previous E- Alerts may be accessed on the* INCompliance website.