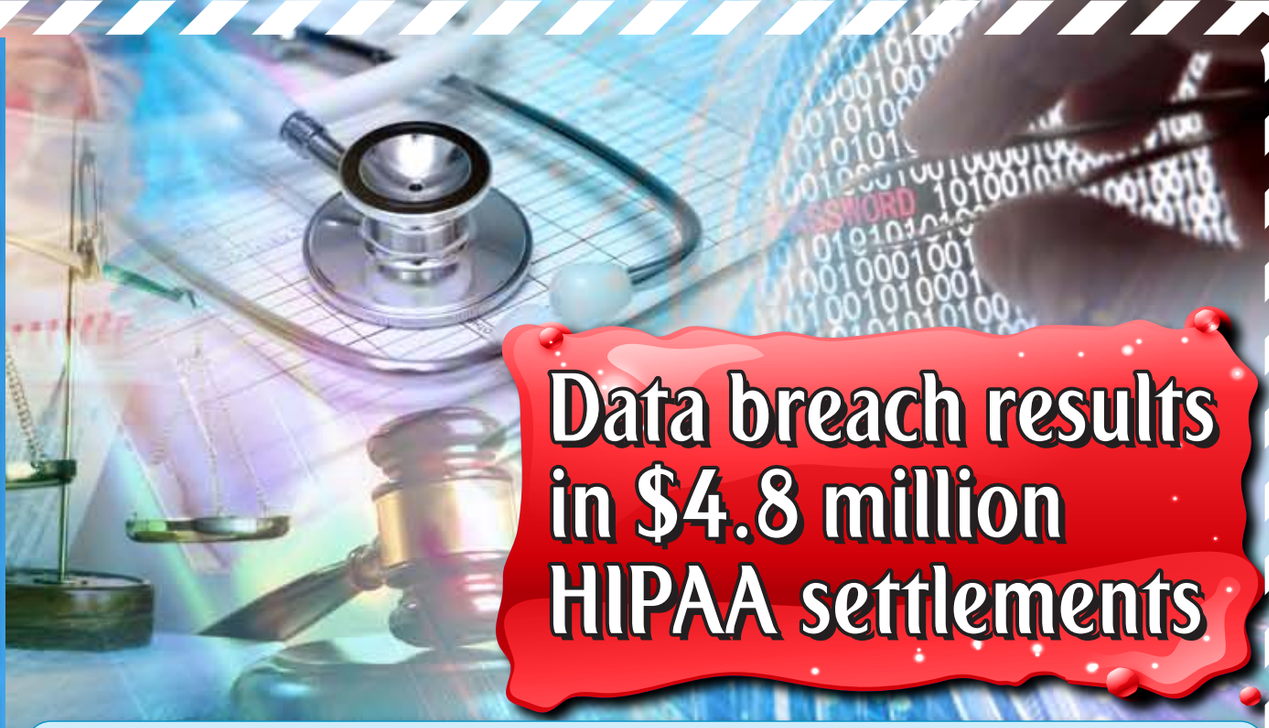
PRESS RELEASE



Data breach results in $4.8 million HIPAA settlements

Two health care organizations have agreed to settle charges that they potentially violated the HIPAA Privacy and Security Rules by failing to secure thousands of patients EPHI held on their network. The monetary payments of $4,800,000 include the largest HIPAA settlement to date.

HHS OCR initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the EPHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.

NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as "New York Presbyterian Hospital/Columbia University Medical Center". NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to NYP patient information systems containing EPHI.

The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient EPHI. Because of a lack of technical safeguards, deactivation of the server resulted in EPHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the EPHI of the individual's deceased partner, a former patient of NYP, on the internet.

In addition to the impermissible disclosure of EPHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP EPHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of EPHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management.

NYP has paid OCR a monetary settlement of $3,300,000 and CU $1,500,000, with both entities agreeing to a substantive corrective action plan, which includes undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing progress reports.

Discuss more about establishing a complete end-to-end HIPAA and HITECH compliance program with leading expert Ali Pabrai. Contact Mr. Pabrai at Ali.Pabrai@ecfirst.com for a complimentary copy of a Checklist for HIPAA Compliance.

"Prime Healthcare and its network of 25 hospitals are excited to have exclusively selected ecfirst, home of the HIPAA Academy, to address HIPAA and HITECH regulatory compliance mandates.

The engagement is based on the ecfirst Managed Compliance Services Program which is a complete end-to-end comprehensive compliance solution that addresses risk analysis, technical vulnerability assessment, policy development, social engineering, business impact analysis, creation of a disaster recovery plan, as well as on-demand remediation services for risk management (corrective action plan).

Prime Healthcare

CHP Certified HIPAA Professional HIPAA Academy

2014 Public Training & Certification Schedule

CSCS™ CERTIFIED SECURITY COMPLIANCE SPECIALIST

June 17-18 | Chicago | June 19-20

Please contact Mr. Pabrai at Ali.Pabrai@ecfirst.com or at +1.949.528.5224

ecfirst

eHIPAA ACADEMY™ HIPAAacademy.Net