

Indiana Security & Privacy Network
Security Subcommittee
Mark Clausman, Chair
mark@sterlyn-group.com

November 17, 2011

St. Joseph Medical Center, Twoson, Maryland

November 5, 2011

Someone stole thousands of X-rays from St. Joseph medical Center. Authorities believe the X-rays were taken for their silver content rather than for identity theft purposes. They contained patient names, dates of birth, medical record numbers, dates of service, physicians, and some diagnostic information. *Information Source:* PHIPrivacy.net

James A. Haley VA Hospital, Tampa, Florida

October 27, 2011

A camera from the Plastic Surgery Clinic was discovered missing in November of 2010. It contained Social Security numbers and photos of patients. *Information Source:* PHIPrivacy.net

OCR HIPAA Audits Finally Kick Off

November 09, 2011 | David Harlow, JD MPH, Principal, The Harlow Group LLC

The HITECH Act called for stepped-up [HIPAA privacy and security and breach notification rule enforcement](#) with respect to covered entities and business associates, to be accomplished by spot-check audits. This month, the first 20 of a planned 150 audit subjects will be getting notices from the U.S. Department of Health and Human Services Office of Civil Rights' contractor, KPMG, saying that their numbers are up. These early test cases will be a proving ground for the auditors and the audit process, as much as for the covered entities to be audited (no business associates in the first 20, or even in the whole batch of 150, apparently). The first round of 20 audits -- and a review of the audit protocols -- is slated to take about five months. Up to 130 other audits will follow, in the final eight months of this pilot. Each audit is supposed to take about 30 business days, and will include on-site interviews and investigations. Document requests are to be turned around in ten days, and KPMG will give 30-90 days advance notice of site visits. In theory, audits may bring to light issues that do not surface in the course of complaint investigations, and are expected to yield OCR guidance and highlighting of best practices. <http://www.healthcareitnews.com/blog/ocr-hipaa-audits-finally-kick>

Military Health Plan Data Breach Threatens 4.9 Million

Tricare says lost backup tapes fall under FTC jurisdiction, not HIPAA, so only offers 90 days of fraud protection.

By [Neil Versel](#) [InformationWeek](#)

October 04, 2011 12:20 PM

A data breach involving nearly 5 million people treated at military healthcare facilities over a 19-year period is raising questions about whether U.S. Federal Trade Commission (FTC) rules supersede Health Insurance Portability and Accountability Act (HIPAA) regulations.

Last week, [Tricare](#), the managed care arm of the U.S. government's [Military Health System](#), disclosed that contractor [Science Applications International Corp.](#) (SAIC) had lost backup tapes containing personally identifiable information--including some

health data--of about 4.9 million people. The tapes contained data from electronic health records (EHRs) used at military hospitals, clinics, and pharmacies in the San Antonio area from 1992 until Sept. 7, 2011.

People affected will not be provided with any private credit monitoring services. "The risk of harm to patients is judged to be low despite the data elements involved," the Tricare notice said. Tricare is directing enrollees to a [FTC site](#) where individuals can place a free, 90-day fraud alert on their personal credit ratings.

"It's clear that Tricare is trying to position this under Federal Trade Commission regulations, not under HIPAA regulations," Ruby Raley, director of healthcare solutions at IT integration and security company [Axway](#), Scottsdale, Ariz., told *InformationWeek Healthcare*.

Unlike HIPAA, FTC regulations don't require entities to sign agreements with "business associates" that hold third parties to the same standards when handling sensitive data. Also, HIPAA regulations require organizations to provide a year of credit monitoring to anyone who may have been affected by a breach. "They're only [offering] fraud protection for 90 days," Raley said of Tricare.

As of Monday, the incident had not been posted on the [Department of Health and Human Services' list of breaches](#) affecting at least 500 people, commonly called the "wall of shame." The 2009 American Recovery and Reinvestment Act calls for covered entities to report major HIPAA breaches to the HHS Office for Civil Rights if the data was not encrypted.

Facebook security breach raises concerns

By [Hayley Tsukayama](#), Published: November 15

A widespread spam attack on Facebook has caused violent and pornographic images to be posted on some users' profile pages, representing one of the worst security breaches in the young Web site's history and raising concerns about its vulnerability to hackers.

The company, which acknowledged the problem Monday, said it was working to shut down the accounts responsible for the attack.

The disturbing pictures surfaced as the company tries to quell concerns about user safety and privacy. Facebook is [reportedly near a settlement](#) with the Federal Trade Commission over complaints about the way it stores and shares user data. Experts said that while this latest attack didn't appear to compromise users' data, it was a serious security breach.

According to Facebook, users were somehow tricked into copying and pasting malicious code into their browser bars. Hackers then gained access to their profiles and could post whatever they wished, and any of the user's Facebook friends could see the images.

Daimon Geopfert, a security expert for RSM McGladrey, said that this was one of the largest Facebook attacks he has seen. The scale and speed were "unprecedented," he said.

Part of Facebook's success has stemmed from its ability to get developers to create games and other applications that work seamlessly on the site's platform. But giving such leeway to outside programmers means the site is also vulnerable to hackers, Wisniewski, a security researcher at Sophos, said.