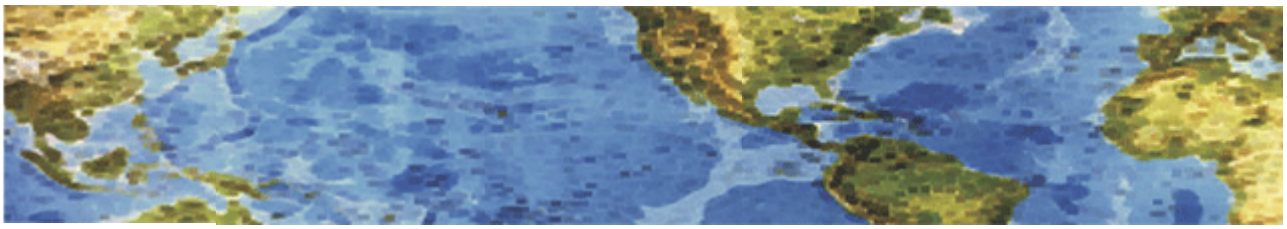
HALL ASSOCIATES



Risk-Based Decision Making Commentary
16 August 2013 Newsletter

At $1.2M, Photocopy Breach Proves Costly

The U.S. Department of Health and Human Services has settled with Affinity Health Plan, a New York-based managed care plan, for HIPAA violations to the tune of $1,215,780 **after a photocopier containing patient information was compromised.** Affinity filed a breach report with the HHS Office for Civil Rights on April 15, 2010, as required by the HITECH Breach Notification Rule.

Affinity officials were informed by CBS Evening News that, as part of an investigatory report, the television network had purchased a photocopier, previously leased by Affinity, that contained confidential medical information on its hard drive. Affinity estimated that up to 344,579 individuals may have been affected by this breach. An HHS Office for Civil Rights investigation indicated that Affinity impermissibly disclosed the protected health information of these affected individuals **when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives**. Moreover, the investigation revealed that Affinity failed to incorporate the electronic protected health information stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

This settlement illustrates an important reminder about **any equipment** designed to retain electronic information: **Make sure that all personal information is wiped from hardware before it's recycled, thrown away or sent back to a leasing agent.** HIPAA covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information. In addition to the $1,215,780 payment, the settlement includes a corrective action plan requiring Affinity to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent, and to take certain measures to safeguard all PHI.

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. That means, "reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information." Additionally, it requires covered entities to address "the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use." For electronic media that means "clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding)."

http://www.healthcareitnews.com/news/12m-photocopy-breach-proves-costly give some more detail on this settlement and http://www.healthcareitnews.com/news/old-it-new-tricks?single-page=true discusses dealing with old equipment in a HIPPA-compliant way.

HALL ASSOCIATES

Cyber Sextortion – Something to warn our kids and employees about

Newly crowned Miss Teen USA Cassidy Wolf is allegedly the latest victim of sextortion. According to the LA Times, the FBI confirmed on Wednesday that it's investigating claims by Wolf and other women who say that their webcams were hacked, photos or video were taken surreptitiously, and that the hacker or hackers then demanded money in exchange for keeping the photos out of public disclosure.

19-year-old Ms. Wolf has told reporters that prior to being crowned, she received an anonymous email from someone who claimed to have nude photos of her, taken via the webcam on her computer. Wolf told Today News that about four months ago, Facebook notified her about somebody trying to log into her account from another state. She then received an email saying that the person had photos of her taken in her bedroom via her computer's hacked webcam. The person, who hasn't been named in the ongoing federal investigation, tried to extort her in exchange for keeping the photos from being made public.

As if everyday webcam hacking weren't shocking enough, this case apparently involves a webcam that was hacked without the telltale camera light coming on to indicate that it was recording. This is how Ms Wolf tells it: "I wasn't aware that somebody was watching me [on my webcam]. The [camera] light didn't even go on, so I had no idea." Note that Some laptops allow you to turn the light on and off in software, others only work physically. So this is certainly possible, if unlikely. But if it's unlikely to suffer a webcam hacking that manages to turn off the camera's "on" light, plain old vanilla webcam hacking that leaves the light on isn't very unlikely at all.

In fact, as the BBC reported in June, there's a thriving black market for access to computers whose webcams have been compromised. Stolen webcam video of females cost $1 per "slave," as they're called. Stolen video of male slaves goes for $1/100 slaves.

If you have a webcam on your computer or tablet, keep an eye on the light. That, evidently, won't stop remote hackers of webcams who manage to turn off the camera light via accessing its software.

But given that such a hack is less likely than one turning on the light, it's still **a good idea to keep an eye on the light. Better still, cover it with a patch - a tiny piece of black tape, say, or a sticker or bandage - when you're not using the camera.** Also make sure your security applications (really, all applications and programs) are up-to-date, routinely clear your browsing history and change passwords into something difficult to guess.

http://nakedsecurity.sophos.com/2013/08/15/miss-teen-usa-2013-says-sextortionist-hacked-webcam-to-snap-bedroom-photos/?utm_source=Naked+Security+-+Sophos+List&utm_medium=email&utm_content=Yahoo%21+Mail&utm_campaign=b434c846c1-naked%252Bsecurity&utm_term=0_31623bb782-b434c846c1-454959897

http://www.latimes.com/local/lanow/la-me-ln-fbi-investigating-sextortion-case-targeting-miss-teen-usa-20130814,0,4440441.story