Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Make Photography And Recordings Part Of Your HIPAA Policies

Plus: Laptop theft places hospital in treacherous waters.

Recent class-action lawsuits have highlighted the extremely expensive consequences of healthcare professionals who photograph or videotape patients inappropriately. If your organization photographs or records patients in the course of providing care, make sure your HIPAA policies contain strong parameters for this.

Johns Hopkins Hospital recently agreed to a $190-million settlement with more than 8,000 patients of gynecologist Dr. **Nikita Levy**, following allegations that Levy secretly photographed and videotaped their bodies in the exam room, according to a July 24 blog posting by Florida-based attorneys **Julie Gallagher** and **Leslie Schultz-Kin** for the law firm **Akerman LLP.**

Although the patients' faces were not visible in the images, "and it could not be established with certainty which patients were recorded or how many, thousands of patients were traumatized, according to lawyers," Gallagher and Schultz-Kin wrote. The patients included both women and girls.

And this is not the only lawsuit involving a physician photographing a patient inappropriately Gallagher and Schultz-Kin point out that several other cases, including some involving posting the photos to social media websites, have cropped up in the past few years.

Beware: "In this era of social media where the use of smartphones and tablets make sharing data so easy, these cases raise fresh concerns about a hospital's ability to protect patients' privacy," Gallagher and Schultz-Kin warned. "Accordingly, it is imperative that hospitals implement comprehensive policies regarding patient photography, video imaging and audio recording."

Best practice: Gallagher and Schultz-Kin advised that such policies should:

- Define allowable purposes and circumstances for obtaining film, digital photographs, video images or recording patients using a camera or other device;
- Set forth standards for the creation, use, disclosure and retention of the images;
- Ensure that patient/legal representative consent is given in writing or by verbal consent documented through an appropriate authorization form; and
- Identify prohibited activities and behaviors relating to photography, video or audio recordings of patients, including personal use, entertainment purposes, posting on social media or in public areas, malicious use, or using such images in a way that is disruptive to patient care or the work environment. Make staff failing to comply with such policies subject to disciplinary action.

Theft Risk Is Always Present: Encrypt All Laptops

Even when a stolen laptop ends up in the bottom of a lake, if you didn't encrypt the device you're sunk.

Case in point: Two intruders broke into the facilities of South Carolina-based **Self Regional Healthcare** over the Memorial Day weekend and stole an unencrypted laptop containing 39,000 patient records, reported partner attorney **Linn Foster Freedman** in an Aug. 1 blog posting for the law firm **Nixon Peabody LLP.**

Law enforcement later arrested the intruders, who admitted to the break-in and theft but claimed they never accessed the information on the laptop and dumped the laptop in a nearby lake, Freedman said. Divers were unable to locate the

laptop. Because the laptop was unencrypted and not recovered, the hospital elected to notify the affected patients.

"The incident reiterates that removable media like laptops should be encrypted at all times when they are within a locked premises, as well as when they are removed from the facility as the risk of theft is always present," Freedman warned.

Doctors, Not Patients, Suffer From Data Breach

In the midst of the many reports of data breaches involving patients' personal and health information, one report stands out because this time it affected physicians.

Blue Shield of California accidentally included 18,000 doctors' Social Security numbers in its required monthly filings to the state **Department of Managed Health Care** (DMHC), according to a July 10 California Healthline report. The filings also included physicians' names, medical group names, business addresses and phone numbers, and practice areas.

The mistake was particularly problematic for the affected physicians because the records were then available to the public under California's public records law, California Healthline reported. Other insurers received the filings, which included the doctors' Social Security numbers, in response to 10 public records requests to DMHC.

Blue Shield sent a letter to the affected doctors promising that the company has instituted additional protections to safeguard against future accidental disclosures of confidential personal information. Although there is no evidence that anyone has used the data for identity theft purposes, Blue Shield and DMHC are offering the doctors a free subscription to a fraud-alert service and one year of no-cost credit monitoring.