Codify
BY AAPC

# General Surgery Coding Alert

## Practice Management: Protect Your Surgical Practice's PHI -- Now More Than Ever

**Let recent breach serve as cautionary tale.**

Did you know that cyberattacks have become more prevalent recently, posing a dangerous threat to the security of Protected Health Information (PHI) that your surgeons gather and store electronically?

Read on to learn about some recent, serious PHI breaches, and to garner some tips from Medicare and other experts about how to protect your practice.

**Cyberattacks Trend Upwards**

A recent hack into a myriad of healthcare partner systems reportedly exposed the PHI of over 650,000 patients across the Midwest and parts of the south.

Due to the significance of the attack, CMS issued a Special Edition MLN Matters release reminding providers to engage with business partners who understand and utilize the best practices compliant with the Health Insurance Portability and Accountability Act (HIPAA). You can access the MLN Matters article at www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/Downloads/SE1616.pdf).

**That's not all:** The Office of the National Coordinator for Health Information Technology (ONC) recently reported that criminal cyberattacks are on the upswing, with an increase of 125 percent over the past five years, "replacing employee negligence and lost or stolen laptops as the top cause of health care data breaches," said **Karen B. DeSalvo, MD, MPH, MSc**, national coordinator for health IT and HHS assistant secretary for Health, and **Nicole Lurie, MD, MSPH**, assistant secretary for preparedness and response, in a joint ONC press release on July 25, 2016. "The average consolidated total cost of a data breach was $3.8 million, a 23 percent increase from 2013 to 2015," they continued.

**Why this matters:** "HIPAA's Breach Notification Rule requires reporting of a breach of unsecured PHI to the individuals and the secretary of HHS and, if a breach affects more than 500 individuals, to the media," explains Michael D. Bossenbroek, Esq of Wachler & Associates, PC in Royal Oak, Mich. "This rule also requires business associates to notify the covered entity as well if they are responsible for a breach. Breaches can lead to HHS investigations and compliance reviews."

**Here's What You Can Do to Protect Your Surgery Practice**

Protect the PHI in your care against healthcare cyberattacks, ransomware, and other digital warfare using the following tips:

- Thoroughly research the background of any and all business partners you associate with and insist upon arranging a HIPAA-compliant business associate agreement (BAA).
- Keep abreast of cyberattack news through the ONC, OIG, and HHS updates.
- Familiarize yourself with the modus operandi of hackers to ensure you can recognize if your patients' PHI has been compromised.
- Immediately report any HIPAA violation of lost or stolen PHI to the authorities. This early outreach may reduce any civil or criminal liability on your behalf.

**Final note:** Although monetary and criminal penalties await a mishandling of PHI breach, that's not all you have to fear.

You also need to "take into consideration the reputational harm to the institution, the loss of public trust, and the potential embarrassment, inconvenience, and harm to patients and their families," Bossenbroek points out.