Compliance Today - December 2018
Year-end review and looking forward: Chief compliance concerns for 2019

by Amit Sarkar

Amit Sarkar (Amit.Sarkar@eyecareleaders.com) is Vice President, IT PMO and Governance at Eye Care Leaders in Charlotte, NC.

- linkedin.com/in/amit-sarkar-compliance-leader

It has been a nightmarish year in many ways for compliance officers in healthcare organizations. The numbers speak for themselves: 1.13 million records were exposed by 110 healthcare data breaches in Q1 2018, and more than 3 million patient records were breached by phishing emails, IT, and unauthorized viewing in the second quarter. Electronic health records (EHR) were hacked, laptops and PCs were inadequately configured, and electronic equipment was mislaid or lost. The Office for Civil Rights (OCR) breach portal[1] indicates that between January 2, 2018, and August 20, 2018, healthcare providers alone reported 104 breaches involving hacking, EHRs, and unauthorized viewing. This does not account for lost equipment, theft, and human error.

Prevention of data loss and breaches should be number one priority

You don't want to be part of the statistics involving healthcare data breaches. The 1,000% leap in health plan data breaches in the first half of the year should be an eye-opener for all connected with healthcare and HIPAA compliance. As many as 884,360 individuals were impacted by 24 breaches involving health plans in the first five months of the year. Data released by the Protenus Breach Barometer[2] indicates that in the second quarter alone, more than 3.14 million patient records were breached in 142 health data breach incidents disclosed to the media or to the U.S. Department of Health and Human Services (HHS).

There's no point in locking the stable door after the horse has been stolen. Therefore, your number one priority in 2019 should be prevention of data loss and of breaches of protected health information (PHI) and electronic PHI (ePHI) through tighter audit controls. It is no longer adequate to have policies and procedures in place. There must be rigorous risk assessment, and risk mitigation to eradicate vulnerabilities as far as is practical to prevent breaches. Reinforcing these measures would be regular audits, especially for the technical safeguards.

Stay out of OIG crosshairs

The U.S. Department of Health and Human Services (HHS) Office of the Inspector General (OIG) periodically reviews the protections instituted by states, and even individual healthcare organizations, to safeguard data they handle. It reviewed Maryland's Medicaid Management Information System (MMIS) and data security in mid-August.[3] You don't want to come under federal scrutiny.