Compliance Today - October 2018
Record retention strategies when systems get replaced

by Shannon Larkin

Shannon Larkin (slarkin@harmonyhit.com) is Vice President of Marketing & Business Development for Harmony Healthcare IT in South Bend, IN.

- linkedin.com/in/shannonlarkin

Most healthcare providers today are at risk, keeping out-of-production electronic health records (EHR) and enterprise resource planning (ERP) systems up and running simply to meet record retention requirements. Although each backstory is a little different, most organizations have at least a small collection of legacy systems — each storing personally identifiable information for patients or employees. Some of these systems were inherited during mergers and acquisitions; some were sunset by the respective vendor; others were simply replaced after failing to meet user production or workflow requirements. These outdated systems were likely built on a variety of platforms and developed sometime over the last 10–25 years. They also likely sit alongside newer "go-forward" EHR or ERP systems that actively manage the current workload, yet don't offer an easy or affordable pathway for consolidating and storing the historical data.

This multi-generational band of legacy EHR and ERP systems collectively is charged with meeting record retention regulations set at agency, state, and national levels as well as HIPAA regulations for privacy and security. Depending on medical specialty or facility type, some records might need to be kept for 25 years or more and, if there is an audit or need to access the data, there often is a tight timetable for producing the information. Efficient e-discovery and release of information can quickly become a tall order, particularly if patient or employee data is stored in multiple systems. More importantly, out-of-production systems — especially those not being routinely upgraded or patched — create risks for system failure and cybersecurity attacks.

It is not surprising that vulnerabilities from aging applications and technologies are the number one concern IT executives cited with respect to cybersecurity in the "2017 Federal CIO Survey" conducted by Grant Thornton and the Professional Services Council.[1] This concern correlates with healthcare ranking number one for cybersecurity attacks for the same year, when it previously hadn't been in the top six.[2]