Compliance Scorecard

Security Leadership Solutions Executive Council

By Eric Cowperthwaite and Marleah Blades

The Hidden Healthcare Security Regulation

Don't forget about the PCI Data Security Standards

Hospitals have a lot of regulation to contend with. HIPAA (Health Insurance Portability and Accountability Act), CMS (Centers for Medicare and Medicaid Services), and Joint Commission requirements all vie for attention and for money, and they all come with frightening penalties for noncompliance. CMS standards impact hospitals' ability to be reimbursed for Medicaid and Medicare services, Joint Commission standards impact their ability to be accredited, and noncompliance with HIPAA means federal regulators breathing down their necks.

But there's another rule they need to be thinking about, one that has slipped under the radar: the Payment Card Industry Data Security Standards (PCI DSS). The PCI DSS were developed by the major credit card companies of the PCI Security Standards Council to facilitate the broad adoption of consistent payment account data security measures. (For information, visit www.pcisecuritystandards.org.)

These standards have gone unnoticed by many healthcare organizations because they don't think of themselves as merchants; but in reality, hospitals make a significant number of credit card transactions for full payment, insurance copayment, for purchases in their gift and flower shops, and for donations to their charitable foundations.

The good news is, several of the requirements of the PCI DSS will already be met in hospitals that comply with the HIPAA Security Rule. Separation of duties, auditing of access to records, and unique identities, in addition to many other elements, are all covered by HIPAA, because both these rules are derived from the same ISO Standards.

The not-so-good news: While HIPAA and the CMS regulations are relatively generic, the PCI DSS are specific. So there are elements of PCI DSS compliance that will require special attention, such as the need to conduct vulnerability scanning of Internet-facing systems and the need to identify where all credit card data is located inside electronic systems.

Hospitals that take credit cards at any level need to acquaint themselves with the PCI DSS and prepare their organizations to comply. For one thing, it's the right thing to do to protect the information of their patients and patrons. For another, it's expensive not to. PCI doesn't set down specific fines for non-compliance, choosing to leave that element to the participating credit card companies themselves, but fines on record have ranged from the thousands to the millions of dollars. That should be enough incentive to give these rules a second glance.

Eric Cowperthwaite is the chief security officer of Providence Health & Services, which has 29 hospitals and more than 50,000 employees located in five western states. Previously, he was the security & privacy officer for Medi-Cal (contracted from EDS), the state of California's Title XIX Medicaid Insurance program, responsible for developing and implementing security and privacy policies, standards and procedures to protect the personal health information of more than 6 million Medicaid beneficiaries. Mr. Cowperthwaite is a member of the Security Executive Council, an international professional membership organization for leading senior security executives spanning all industries, both the public and private sectors, and the globe.

Marleah Blades is senior editor for the Security Executive Council, which maintains a large and growing list of laws, regulations, standards and guidelines that impact security (https://www.securityexecutivecouncil.com/public/lrvc). For more information about the council, visit www.SecurityExecutiveCouncil.com/?sourceCode=std.

time, data-rich reports to inspectors. The hospital, like most medical facilities around the country, relies on JCAHO accreditation procedures for meeting quality standards, so accuracy and clarity are key when it comes to providing this information.

"The big thing is the documentation — to show we're actually doing what we say we're doing," Alexander says. "For example, we have one generator getting live data fed to the Honeywell system at different peak and load times, and the printouts help us provide information that meets the requirements and standards that apply to generator use."

A $25 million expansion of the hospital's 14-acre facility is planned for the next few years.

In addition to compliance, the generators' live feed to the EBI system also enables the hospital to proactively resolve issues before they become critical. With hospital surgeries lasting up to 13 hours, generator maintenance is essential to keep all systems up and running properly in case of power failure. The live feed enables personnel to monitor and track critical factors such as temperature, voltage output and machine runtime, allowing for better maintenance practices and system management.

More on the Horizon

The hospital is planning an estimated $25 million expansion of its 14-acre facility over the next several years. EBI will manage HVAC equipment for two new sections of the hospital, and what's left of the hospital's existing control system will be integrated onto the centralized platform.

The ability to control everything from one location will enable the hospital to implement energy management strategies, for example, and further expand the ways in which it saves time and money. "We'll start to see savings on natural gas, on electricity, even on water," Alexander says. "We'll be able to better manage and control our energy use with real-time information, and it will help us make better decisions on our utilities going forward." STD