The EHR imperative
Eliminating outages and combatting cyberattacks can help improve patient care
Introduction

The complexity of healthcare is evident in both the practice of medicine and health information technology (IT). The push from inpatient to outpatient settings and the shift from volume to value-based care adds to this complexity by contributing to market disruption in the form of mergers, acquisitions, and expansions. Healthcare organizations currently face a significant challenge when integrating systems and processes across the care continuum.

Electronic Health Record (EHR) systems have become a mission-critical component for delivering appropriate and timely high-quality care. They function as the single source of truth for providers and patients. Healthcare providers need their EHR and supporting infrastructure to be always running and compliant with strict regulations for health data security and privacy.

At the recent annual meeting of the Health Information and Management Systems Society (HIMSS) in Las Vegas, the Centers for Medicare and Medicaid Services (CMS) stressed the importance of EHRs and health data privacy and security to two Medicare programs, Promoting Interoperability (formerly the EHR Incentive Programs) and the Quality Payment Program.

“Ensuring the security of healthcare data will be an absolute requirement to avoid negative payment adjustments or receive an incentive payment,” said CMS Administrator Seema Verma. These additional penalties come on top of steep costs to a healthcare organization suffering from a data breach, which averaged $3.62 million per organization according to a 2017 global study.

Now more than ever, chief medical information officers (CMIOs), health information managers (HIMs), and IT staff need visibility into the many touchpoints spanning a network of care sites. They need to be able to keep tabs on potential internal and external factors affecting the optimal performance of EHR systems, especially given the rise in number and complexity of cyberattacks.

EHRs: An attractive target for cyberattackers

The valuable information stored in a patient’s electronic record has not gone unnoticed by individuals looking to profit from the sale of financial and personally identifiable healthcare information (PHI).

“Healthcare is an attractive target,” said Craig Gormé, IT Security Manager at University of Florida Health, at HIMSS18.

“Along with this complex landscape we have to deal with, the attackers have unlimited time and unlimited resources,” he continued. “They are constantly attacking our networks and our people. They are continuously conducting phishing attacks and reconnaissance against our systems, throwing in malware attacks. We are always behind the eight ball.

The motivation for attackers is a simple one—money.

“Records are money,” Gormé stated. “Each record today can cost about $50 on the dark web. If you get compromised, you lose thousands of records that contain credit information, Social Security numbers, and insurance information. Last year, criminal organizations made over $172 billion attacking healthcare systems and more.

“Cyberattacks can assume many different forms, from attempts to penetrate systems by exploiting unpatched vulnerabilities in health IT systems to phishing

—Craig Gormé
IT Security Manager
University of Florida Health

“Ensuring the security of healthcare data will be an absolute requirement to avoid negative payment adjustments or receive an incentive payment.”

—Seema Verma
CMS Administrator

Each record today can cost about $50 on the dark web. If you get compromised, you lose thousands of records that contain credit information, Social Security numbers, and insurance information. Last year, criminal organizations made over $172 billion attacking healthcare systems and more.

—Craig Gormé
IT Security Manager
University of Florida Health
Prioritization is the key to remediation because it’s nearly impossible to fix each and every problem.

A proactive approach to health data security

Understanding the attraction of bad actors to sensitive health data should lead organizations to rethink their approach to health data security. In a presentation on the value of penetration testing, Duke Medicine Chief Information Security Officer (CISO) Chuck Kesler, and CynergisTek Vice President of Cybersecurity Strategy John Nye echoed the sentiments of Gormé and emphasized the need for healthcare organizations to be on the offensive.

“Right now, we are very reactionary and it’s really, really hard to get out of the reactionary mode of security. But we have to start looking and finding these issues before the bad guys do. So rather than waiting until a breach happens, let someone who is not going to use that breach to his advantage find those holes, tell you about them, and start fixing them,” said Nye.

A proactive approach to health data security is two-pronged: surveillance and remediation. The ability to effectively monitor threats requires visibility into the many endpoints that comprise the organization’s entire infrastructure. However, organizations will not be able to gain this insight unless data feeds are organized and displayed coherently and concisely to key IT staff.

Visibility is only the first step toward remediation. According to Kesler, threat vectors and vulnerabilities must be addressed in order of priority. Prioritization is the key to remediation because it’s nearly impossible to fix each and every problem. That means looking at the results of vulnerability scans and assessments and prioritizing and responding to security incidents and vulnerabilities that would have the greatest impact on the security of your organization first.

Buy-in from the top levels of the organization is likewise vital to making tough but necessary decisions around a cyber response plan. Taking a proactive approach to cybersecurity response is the best way to prevent minor threats from becoming major ones.

“You want to stop the bleeding. You must integrate your business leadership into the security incident-handling process to help decide if you need to shut down or block a critical piece of business infrastructure,” UF Health’s Gormé advised.

Combatting threats and maintaining uptime

In addition to malicious attempts to take down critical systems, EHRs and other health IT infrastructure that perform above or below appropriate thresholds can also lead to system outages. A comprehensive view of a healthcare organization’s IT infrastructure and the impact of these outages on critical services is essential for delivering a great patient experience.

“How if you don’t have complete visibility into the impact of outages on business applications, teams, and infrastructure, or have the ability to bring disparate teams together through automated workflows to rapidly resolve these issues, you can adversely affect patient outcomes,” said ServiceNow healthcare solutions expert Christopher Killion.
Using an IT operations management solution that automates service mapping helps with getting complete service visibility. It lets healthcare providers get to the root cause of business service issues, instantly see the business impact of planned changes or outages, and easily optimize the architecture of critical business services, reducing costs and improving reliability.

For ServiceNow Healthcare Chief Architect Drew Koerner, helping provider organizations strike a balance between system performance and security is critical. By optimizing the infrastructure in this way, clinicians are able to provide efficient and effective care to patients while using their EHR and other health IT systems.

“By combining the power of ServiceNow IT Operations Management and ServiceNow Security Operations, healthcare providers can rapidly prioritize and resolve issues, be it outages or security threats,” he explained.

“ServiceNow IT Operations Management maps everything that happens to the various components within an Epic environment—for instance, the cache servers, hyperspace, and presentation tier—to the actual workflow response slowness. Information is then routed to the appropriate application owner or infrastructure team to remedy the situation since the software knows specifically which workflow is slowing down.”

The ability to pinpoint and respond to security incidents and vulnerabilities on the network, within individual systems or elsewhere proves an equally powerful tool in combating cyberattacks.

“For instance, we identify an attack on one of the systems. It is a phishing attack that targeted email servers. From the email servers, hackers go to the active directory and then on to the SQL servers. We can trace that activity and make sure that we are correctly responding to the right components and right pieces,” Koerner details.

The creation of a configuration management database (CMDB), a record of all IT assets in the form of configuration items (CIs) provides additional benefits. These assets include hardware, software, networks, location, documentation, and personnel.

“An integrated services dashboard allows you to see the status of business services and the IT services that support them,” Koerner noted. “It lets you identify high-priority events that are likely to impact business services in the near term and drill down to the relevant CIs. You can see existing problems that are causing outages and potential problems before they cause service downtime.

The end goal is helping providers keep their mission-critical systems online to ensure patient care isn’t impacted.

“Healthcare providers can, not only prioritize the assets, but also the vulnerabilities they need to focus on first, based on how critical those assets are to a patient care process. And they can respond to these issues and threats by combining the power of ServiceNow IT Operations Management and ServiceNow Security Operations,” Koerner concluded.
Conclusions

Health IT systems support clinicians in the delivery of high-quality care. When they go offline and data becomes unavailable or compromised, these systems can instead prove a serious hindrance, especially when EHR technology is one of those affected systems.

As healthcare organizations expand and support more complex services and technologies, their IT leadership will face increasing challenges in keeping critical systems operational and sensitive data secure from bad actors.

By combining the power of ServiceNow IT Operations Management and ServiceNow Security Operations, healthcare organizations can pinpoint and remediate service outages as well as security incidents and vulnerabilities impacting components of their IT infrastructure fast—and ensure that patients receive the best possible care at the point of service.