KPMG

Access is power

Access management may be an untapped element in a hospital's cybersecurity plan

January 2016

kpmg.com

Introduction

Patient data is a valuable asset. Having timely access is critical for doctors and clinicians providing care and as a means of ensuring patient safety. However, there is another constituency that wants to get its hands on patient data: Cyber criminals.

Access management and the accompanying processes, controls and technologies are about getting the right people the right access to the right information at the right time. Without it, none of the following would be possible:

- ✓ Use of Electronic Health Records (EHRs) to take patients' medical histories into account
- ✓ Patient engagement with their own Personal Health Information (PHI)
- ✓ Improved quality of care and real-time quality measurement
- ✓ Sharing of patient data to coordinate care across settings
- ✓ Cloud enablement, mobile health, telemedicine, and virtual care
- ✓ Certain patient safety measures

Hospitals are performing a difficult balancing act, however. On the one hand, they want to streamline access to patient data and allow data to be fluid throughout the organization in order to achieve the better outcomes demanded by law. On the other hand, all this increased access is raising the risk of data breaches, hacks and leakages – cyber events that could put an organization's long-term financial and reputational health at risk.

*Report based on data from a quantitative survey of 223 U.S.-based healthcare executives, including chief information officers, technology officers, security officers, and chief compliance officers.

Hospitals are not blind to these risks. In the recent "2015 KPMG Healthcare Cybersecurity Survey," 44 percent of hospital respondents cited financial loss as their major concern in the event of a breach, while 39 percent said they were most concerned about damage to their reputations.

Access is a mixed blessing

Although access is critical to raising quality and outcomes, it is important to remember that almost every major cyber event over the past decade has in some way or other targeted gaps around access controls and privileged user access. According to a recent HIMSS survey, 64 percent of respondents were attacked by an outside entity in the last year[1].

And there is virtually no limit to the damage a data breach can cause. Once cyber-criminals gain privileged users' credentials, they can escalate access and lie in wait for the data they want to steal or gain privileged access they don't warrant[2].

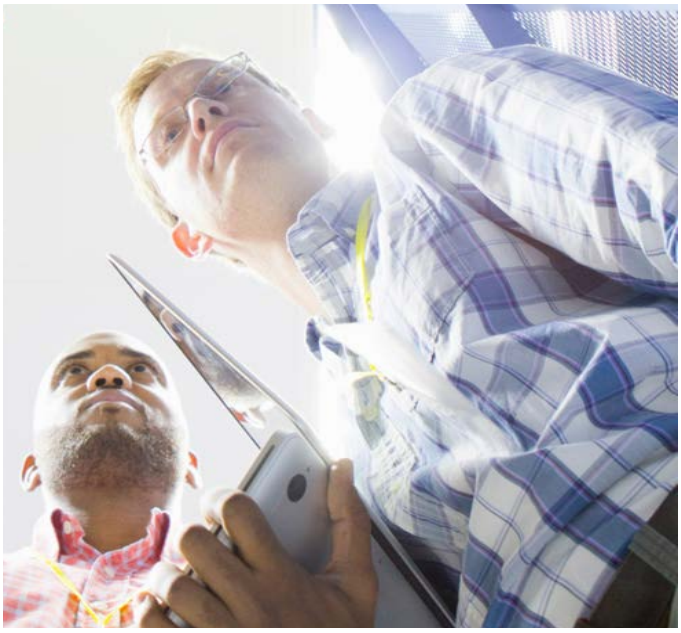
Cyber-crimes can include: copying proprietary innovations and new uses of medical technology; holding medical devices "hostage" until a ransom is paid; and stealing increasingly valuable Personal Health Information (PHI). PHI often includes full medical records, social security numbers, credit card information, billing and insurance forms, and prescription details, all of which contain personal identifying information that can be used to perpetrate medical and financial identify theft. PHI in particular is sought after by criminals because the data cannot be as easily changed, thus giving it a value on the black market up to ten times that of credit card information.

Hospitals are compelled both by law and self-interest to invest in and develop technologies that use patient data to improve connectivity, patient care and population health. However, they are not keeping pace with technologies and programs that protect that data from unauthorized access. In fact, technology solutions used in healthcare settings should be designed with security concepts and controls built into EHR software, clinical systems, medical devices, and mobile technology. Unfortunately, the burden of this usually falls to provider organizations themselves, which have historically been ill-equipped to address and integrate complex security and architectural requirements across so many disparate platforms. Astonishingly, only 52 percent of hospital administrators are prepared to handle a data leakage event, according to the KPMG survey. If left unaddressed, the risks will only escalate.

Safeguard the entry points

It is not just irresponsible or malicious behavior that can cause a data breach. Legitimate, every-day actions of hospital employees can raise risks as well. For example, providers accessing patient records during a medical emergency might borrow another provider's privileged access, thus creating an entry point for a breach. Doctors might access patient records offsite via a computer or mobile phone. EHRs might be sent to another physician for a second opinion, creating an entry to the network. HIPAA-compliant texting between patients and physicians, telemedicine via smartphone and computers, remote monitoring software, and smart devices implanted into patients all represent "attack vectors" for cyber criminals, according to a recent report from the SANS Institute[4].

Of course, these risks increase with the number of users seeking access. Respondents to the KPMG cyber survey broke down as follows: Thirty-nine percent had 1,000-5,000 employees, 20 percent had 5,000-10,000, and the largest organizations, which face the largest threats, had more than 10,000 employees.



Hospital administrators seem to have a basic understanding of the level of risk they face from access-related issues. According to KPMG's cyber survey, hospitals stated that their biggest vulnerabilities were "sharing information with others" (47%), employee breaches (35%), and wireless computing. Healthcare organizations need to elevate access control protocols to the executive agenda. According to Cisco Systems:

44 percent Almost half (44 percent) of employees admit that they share work devices with others without supervision.

39 percent 39 percent of IT professionals reported dealing with an employee accessing unauthorized parts of a company's network or facility.

18 percent 18 percent of employees share passwords with co-workers[3].

Repercussions beyond IT

Many hospital executives believe access management is simply an IT issue. In reality, data leakage and breaches due to poor access management controls can have repercussions throughout an organization. These events can lead to significant fines, loss of reputation and heightened regulatory and public scrutiny, all of which can cut into already thin profit margins.

Financial damages from data breaches in the healthcare industry amount to $6 billion annually, with an average price tag of $2.1 million per organization, according to the recent "Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data" from the Ponemon Institute[5].

Patients do not take data breaches in stride, as the damage to individuals can be all too real. Of those who have had their medical records stolen, 69 percent will have sensitive medical information disclosed, 44 percent will be at increased risk of financial identity theft, and 23 percent run a greater risk of medical identity theft, according to the Ponemon study[6]. This last is particularly frightening. The average amount of money patients spend to restore credit and pay fraudulent healthcare charges is $13,500[7]. The study further states that half of all patients would change healthcare providers if their medical records were compromised[8].

And it can be challenging to comply with government mandates. For example, HIPAA's "Minimum Necessary Requirement" rule states that "covered entities [must] take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose[9]." The problem is that organizations have not put in the effort to specify what "minimum necessary" means for different users, thereby adding the risk of compliance violations to the risk of a breach.

Access management methodologies

Some hospital administrators seem to believe that addressing these issues is as simple as creating policies about password sharing, immediately removing terminated employees from the network, and adding security software to wireless routers. However, this is not enough. Solutions need to be codified into company policies and protocols.

Two of the most important steps hospitals should take are applying role-based access methodologies and tightening access entitlements. Many healthcare organizations have a large number of operational functions or roles with overlapping access. For example, there may be hundreds of hematology nurses, all of whom require the same access to the same type of information. Access allocation by role or function can help organizations quickly and effectively manage how access is provisioned to large groups at one time.

Far too many organizations, particularly in healthcare, are only focused on limiting the number of privileged accounts they authorize for access. Cyber criminals can gain access to networks by compromising privileged users' credentials and then using that access to extract large amounts of data. Therefore, it is important to have stringent controls in place to monitor these privileges across applications, servers, infrastructures, firewalls, routers, and more.

And when it comes to managing those with more operational, back-office roles, including some vendors, organizations should institute entitlements that allow access to specific data but with tight restrictions, including proscribed uses and timeframes.

Hospital administrators seem to understand the risks that come from third-party vendor access. Of the respondents to KPMG's cyber survey, 74 percent "agree" or "strongly agree" that third parties represent a significant risk to data security. And 84 percent of them evaluate third parties' information security postures as part of their due diligence before entering into a business relationship. And yet, it is still alarming that only 35 percent have programs in place to protect against vulnerabilities stemming from vendor access to sensitive data, according to the survey.

An organizational Imperative

In order to develop a robust, flexible and sustainable Access Management program, organizations must first spend time developing strong governance structures, effective controls, and efficient processes to support them. And this will require the participation of organizational functions beyond IT, especially the senior management team and community user groups.

Roles and their related data requirements need to be mapped, which requires input from human resources and clinical teams. Rules and controls must be developed in a coordinated effort with staff responsible for legal, compliance and risk management issues. Clinical departments will need guidance on how to monitor and manage certain combinations of access privileges. And the entire process must be traceable so that, in the event of a breach, damage can be contained through a rapid audit of the system and access allocations.

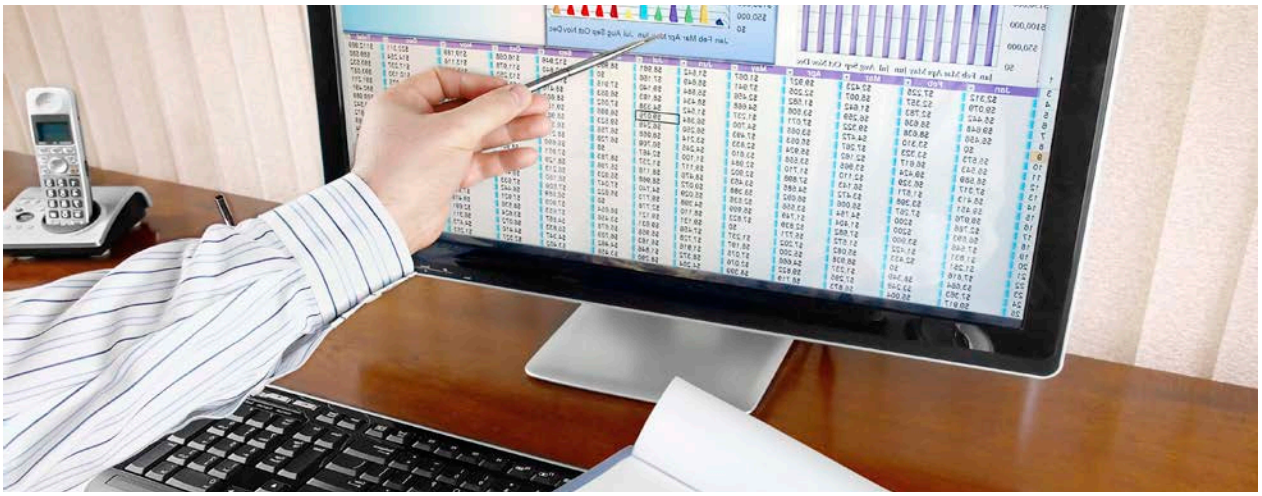
Ultimately, a wide range of stakeholders must buy into access management controls to ensure that the approach meets the needs of the business, both in terms of rigor and flexibility.

KPMG understands access management

There are a number of potential technology solutions vying to capture the healthcare access management market. However, more than software is needed to protect an organization from cyber-attack. For example, KPMG's Cyber Solutions deliver additional value in terms of industry experience, data and analytics, audit traceability, connectivity back to the specific requirements of HIPAA and the Omnibus Rule, and, of course, deep identity access management software implementation experience.

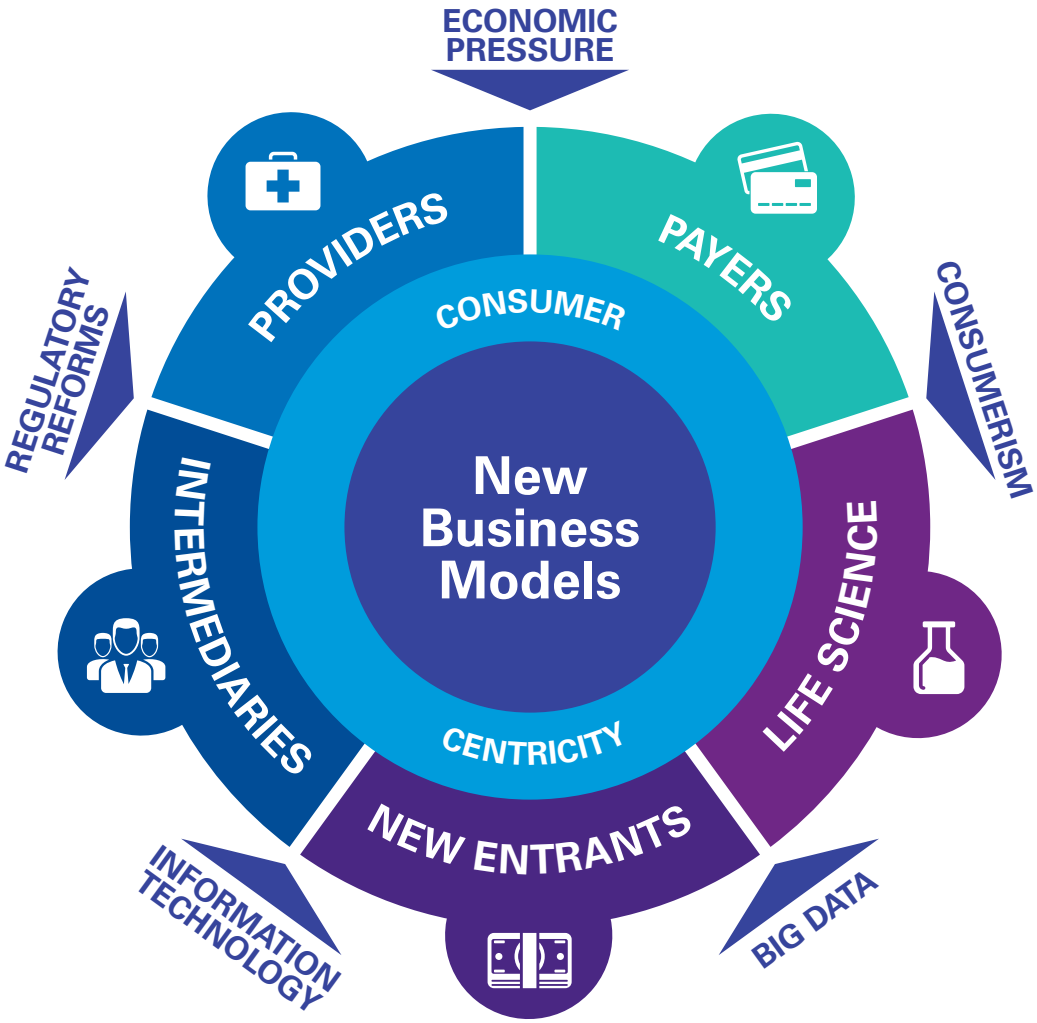
The challenge is that – when applied to a poorly designed process – a solution can accentuate and accelerate the risk. Therefore, we often advise our clients to begin by reaching for clarity on the process and strategy they intend to take. Only once these foundational elements are in place should they start thinking about how technology can be leveraged to improve efficiency and ongoing monitoring.

A strong foundation for access management is not only about better security and compliance. It is about reaching better insights into clinical and business workflows that improve care. And once these have been identified, it becomes rather straightforward to search for inefficiencies, make more strategic investments in technology, and analyze how to safeguard organizational and patient data.



1. Weinstock, M. (2015).Cyber wars and the battle for patient care, *Hospitals & Health Networks Magazine*.
2. Hagerman, K. (2015).What's next for privileged access management? *Healthcare IT News*.
3. Kern, C. (2015).Best practices for privileged access management in healthcare, *Health IT Outcomes*.
4. Filkins, B. (2014). New threats drive improved practices: State of cybersecurity in healthcare organizations SANS Institute.
5. Ponemon Institute (2015).Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.
6. Ponemon Institute (2015).Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.
7. Ponemon Institute (2015).Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.
8. Landi, H. (2015).Data breaches could cost providers $305B in lost patient revenue, *Healthcare Informatics*.
9. U.S. Department of Health & Human Services (2015). Minimum Necessary Requirement, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html

Our perspective



About KPMG HCLS

KPMG LLP is a leader in convergence, helping organizations across the healthcare and life science ecosystem work together in new ways to transform the business of healthcare.

KPMG's Healthcare and Life Sciences practice, with more than 2,000 partners and professionals supported by a global network in 155 countries, offers a market-leading portfolio of tools and services focused on helping our clients adapt to regulatory change; design and implement new business models; leverage technology, and data analytics to guide them on the path to convergence.

Contact:

Michael Ebert
Partner, Healthcare & Life Sciences
T: 267-256-1686
E: mdebert@kpmg.com

kpmg.com/socialmedia

kpmg.com/app