SECURITY

Of Special Interest To Health Data Centers

Secure Medical Records

Electronic Access Means Privacy Challenges For IT

by Christian Perry

• • •

Technology's incessant drive toward flexibility and ease of use occasionally brings with it a catch-22. Perhaps nowhere is this more evident than in the medical field, where the continuing implementation of electronic medical records is simultaneously improving patient data management and creating potential security leaks. Although medical records systems are inherently secure for the most part, facilities nonetheless face the constant threat of theft from insiders.

"While hospitals and other health organizations go to great lengths to protect patients' health information, the risk is still present that this information may be viewed or distributed inappropriately," says Michael Bilancieri, director of product management at Imprivata (www.imprivata.com). "Whether it is due to accidents, mistakes, or malice, the possibility exists that even secure environments could have a breach."

Threat Identification

Potential threats to the privacy of medical records are certainly not a new problem. As Martin Hack, executive vice president of NCP Engineering (www.ncp-e.com), notes, anyone in the past with access to paper charts and file cabinets could examine patient files, but now patient information is spread through provider networks, insurance companies, and other parties who work with patient health information. As a result, the threat has morphed into one that's far more complex and significantly harder to control.

"The biggest challenge is probably differentiating between what's legitimate access and what's not," Hack says. "Healthcare is a highly dynamic environment, and someone who has access to records may not [have access] three months down the road, and the [remote] access management system has to be able to account for that. And on top of that, there's a huge amount of data within the providers' own systems and other covered entities that they might share the data with. Being able to connect securely and easily between these organizations should be a top priority."

The balance of easy access and security represents a constant battle for IT personnel in the healthcare field, who must interact with medical professionals who might not completely grasp the extent of potential threats. Part of the challenge, according to Bilancieri, is identifying where PHI (patient health information) might be at risk, such as removable storage devices that can limit the controls IT departments have over data. The increased use of mobile devices, such as smartphones and tablets, to access systems (and not always in a managed way) further complicates the task of controlling and managing data.

In this instance, monitoring tools that report on user access to EMR and other systems that contain PHI can help illuminate potential unauthorized access and other privacy-related problems. Bilancieri also recommends locking down endpoints to prevent data from being copied to external or removable devices, which can be lost or stolen, and implementing solutions that enable strong authentication (rather than just simple passwords).

Act On Access

Without thorough planning and policy enforcement, the prospect of effectively protecting patient data is weak at best. Access—and the ability to prevent it—is the most critical factor when developing a strong data protection strategy, and how you approach access will go a long way toward your future security. Kurt Johnson, vice president of strategy and corporate development at Courion (www.courion.com), notes that an access assurance strategy ensures the right people have the right access to the right resources and are doing the right things with them.

"The key to protecting sensitive patient information from insider threats is defining, assessing, enforcing, and verifying strong access control policies to EMR systems and other corporate assets. This is often a challenge for IT professionals in the healthcare industry, as staff turnover can be frequent, employees' roles are constantly changing, and there is often a high level of contract work being performed. On a daily basis, hundreds of user accounts may need to be set up, changed, or disabled," Johnson says.

However, the expectations that providers can effectively manage patient-level access are likely too high, warns Tom Loker, COO at Ramsell Holding (www.ramsellcorp.com). Even when access lists are created, rules are applied, audits are run and reviewed, and unauthorized access is discovered and potentially prosecuted, these steps are only as effective as the diligence of personnel administering the systems, he says. Further, he argues that today's systems are limited in terms of their inherent security, although more secure systems based in the cloud are on the way.

"Another significant challenge is frankly the lack of understanding as to the real threats and the true benefits of the systems themselves, and who should actually be in charge of the records and their distribution," Loker adds. "Some believe that the systems need to be insurer- or payer-focused. Others believe they should be provider-focused, and many more are coming to the belief that they need to be patient-focused. The patient, as the ultimate buyer of the services, needs to have the systems designed and implemented so that they are the arbiter of who gets to be in their virtual care group and who gets to see what."

Loker recommends that privacy officers engage in constant and thorough training on emerging technologies, particularly because many were trained primarily on prior paper-based systems. Further, he says, some of these officers juggle real risks to their livelihood, economic liability, and reputations should a breach occur with the ever-increasing demand for access from patients, providers, insurers, and government authorities. Simply erring on the side of maximum security, Loker warns, will leave the benefits of EMRs on the sideline. "Privacy officers need to be able to compare the risks against the savings and then be in a position to proactively and effectively educate their constituents and provide effective systems that put the patient in control and actively responsible for their own privacy," he says. P

Key Points

- The rise of electronic medical records can create a complex, tough-to-manage ecosystem for personnel charged with protecting patient privacy.
- Identifying where and when patient health information is at risk through the use of monitoring tools can help keep records secure.
- The creation of thorough, stringent policies is critical to ensuring the right people always have the right access to patient information.

Policy Planning

Creating a policy that protects sensitive patient information from unauthorized users while providing proper access to authorized users is a crucial strategy for any medical facility. Kurt Johnson, vice president of strategy and corporate development at Courion (www.courion.com), outlines the following steps for developing this type of strategy.

- Define a user access policy that allows or restricts access according to authorization level.
- Assess how user access and activity affect risk.
- Enforce automated access policies on an ongoing basis to prevent unauthorized access to sensitive information.
- Review user access policies on an ongoing basis to determine who has access to what sensitive data.
- Verify that current access is appropriate and in compliance with both corporate and industry regulations (remediate access when it is not).