HOW CLOUD SECURITY CAN PROTECT PATIENT DATA FOR MEDICAL GROUPS
Breaches that exposed celebrity photos, sensitive corporate e-mails and private consumer information understandably leave many people anxious about data security. Hunkering down in fear about a potential breach may seem like a natural response. However, a certain amount of anxiety about data security can be healthy — especially if it motivates medical groups to act and fortify their data protection.

Securing sensitive patient data presents its own set of challenges – even when medical groups enact their own policies that go beyond HIPAA minimums. When it comes to your health IT, what’s the best approach against internal and external security threats – both now and in the future?
CLOUD-BASED VS. ON-SITE STORAGE: THE BASICS

Some may be surprised to learn that storing all your clinical and financial data on servers somewhere in the office – under a desk or in a closet – may not be the safest approach. Yes, it’s reassuring to see and touch the servers, but on-site hardware can be vulnerable to both theft and physical damage.

Increased data security was one reason that Eppel Family Medicine in Port Orchard, Wash., chose a cloud-based EHR. “We didn’t want a server that could be stolen,” Ken Adams, office manager, stated. “The cloud system was definitely a draw right from the get-go. Even more than the cost and ease of use, we didn’t want it here in the office. We wanted somebody else to protect it from the bad guys.”

Moving your data to the modern defenses of the cloud can raise the level of protection. But how can that be?

This report explains the ways that a reputable cloud vendor can enhance the security of your sensitive financial and clinical data, whether you’re a small practice, large medical group, or enterprise health system.

BENEFITS OF THE CLOUD

Protecting personal health information is probably only one of your practice priorities. Paying attention to patient care, staff productivity and the overall success of your business can leave you little time to commit to data security. A cloud vendor can bolster your current and future protections.
Many practices choose cloud security because:

**benefit #1**

GOING IT ALONE CAN BE MORE COSTLY.

Most cloud-based vendors physically store information in highly secure data centers. Armed security guards, motion activated cameras and many additional protections make these large, dedicated centers more secure than smaller storage facilities or medical offices. Also, some vendors include the cost of data security in their ‘software as a service’ pricing. If security is not included or their pricing doesn’t seem transparent, make sure to ask.

Cloud security vendors “allow healthcare providers to have the best security measures in the industry without the capital investment otherwise required. You can better use these resources to provide patient care,” says Josh Siegel, Chief Technology Officer at CareCloud.

**benefit #2**

THEY GET AN EXTRA LAYER OF PROTECTION

Beyond physically protected data centers, many cloud security firms or hosting companies manage and protect sensitive information. Amazon Web Services (AWS), for example, “provides a reliable, scalable and inexpensive computing platform in the cloud that can support healthcare customers’ applications in a manner consistent with HIPAA and HITECH.”

In other words, in addition to their own security protections, many cloud vendors also partner with global web security firms. These larger companies monitor for threats emerging worldwide and provide an extra layer of data security for medical groups, often for no additional fee.

68% The percentage of healthcare data security breaches from lost or stolen files
23% The percentage caused by hacking
Data security breaches, by their nature, come unexpectedly. How quickly you respond can make the difference between reassuring patients and sending out the dreaded e-mail announcing compromised personal information.

Cloud security firms can provide immediate and ongoing threat detection. “We’re using Alert Logic Threat Manager. It detects vulnerabilities and makes recommendations,” Mr. Siegel says. “It’s proactive, real-time protection.”

Ultimately, securing patient data remains your responsibility, but you don’t have to go it alone. Cloud security firms generally employ teams of security professionals to look for these threats. Importantly, these experts can gauge the severity of a threat and address the danger themselves or tell you what actions you need to take to protect yourself.

Cloud-based EHRs can be as secure as online banking, stated Ronald Manke, a regional director for the New Jersey NH-HITECH Regional Extension Center. The extension center recommends smaller medical groups, in particular, adopt a cloud-based EHR to take advantage of the additional technical expertise. He added that about 60% of the center’s nearly 8,000 groups with 3 or fewer physicians select a cloud-based EHR.

Cloud security is not just geared for smaller medical practices. The additional expertise can help enterprises and larger medical groups too.

“Arguably the biggest security risk in any infrastructure is overlooking serious security flaws because of time, expertise and resources. No system is perfect, and the reality is that a well-staffed cloud provider, with highly-trained staff dealing with security every day, is often likely to reduce the chances of security breaches occurring, compared
to an overworked and under-resourced corporate IT department,” Rich Quick writes in a post for TNW (The Next Web). “It’s a simple economy of scale. A cloud host is more likely to have robust and well-configured load balancers, firewalls and up-to-date patches than an average enterprise, as it’s the focus of their business.”

**PLAYING YOUR ROLE IN PRACTICE DATA PROTECTION**

Firewalls, strong password policies and user education remain vital to keep your software secure on the practice- or medical group-user level. Microsoft, Google, and LifeHacker each recommend ways to create a strong password. Also, avoid over-reliance on a site’s “strength meter” when creating a password, Concordia University researchers warn. The same passwords rated different strengths on different sites, suggesting no reliable industry standard exists.

Protecting your data is about more than infrastructure and technology, Mr. Siegel says. “The Practice Administrator plays an active role in ensuring the access policy and user behavior are in line with regulations.”

**BENEFITS OF THE CLOUD**

When you’re ready to choose cloud-based security, you can narrow down your vendor choices by asking the following 3 questions:

1. **Where do you physically store my data?**
   Ask specific questions about number and location of primary and additional facilities. Also, do they store and protect information in at least a “Tier 3” or higher data center?
How do you replicate my data?
Data replication or redundancy can be an important safeguard in the event of a natural disaster or other event affecting one data center site.

What security protections do you provide?
Many cloud-based companies use software security firms, like Alert Logic or FireEye, to manage and secure the data at the network and hardware level. Ask your vendor any specific questions you have.

If you’re unhappy with any of their answers, keep searching for a cloud-based vendor you feel you can trust. Taking proactive measures now to strengthen your data security can pay off in the long run.

“In order to make a secure and smooth transition [to the cloud], studying all the security requirements regarding the privacy and confidentiality of patient data are essential,” suggests Joel JPC Rodrigues, PhD and colleagues in their study of cloud EHR security and privacy issues. “Cloud clients should demand total transparency from the Cloud service provider. Knowing this kind of information is critical to being able to choose the most suitable provider for the client’s needs.”

SECURITY AND GREATER COORDINATION OF PATIENT CARE

Protecting electronic health record data privacy while promoting greater interoperability among different systems is a main priority for Lucia Savage, Chief Privacy Officer at the Office of the National Coordinator for Health IT. Cybersecurity remains one of the biggest obstacles to the secure exchange of health information, she stated.

“I think people are very concerned about [cybersecurity], and rightfully so. Those of us who work in the industry have been waiting for what happened to Anthem [in February 2015] to happen,” she told the Journal of The American Health Information Man-
agement Association. “We knew that a large health company was going to get hit, we didn’t know when or where.”

Later the same month, a fire at a large Brooklyn warehouse used for storage by many New York City hospitals revealed the vulnerability of paper medical records. These events raise the opportunity to discuss cloud computing as a potential solution, Ms. Savage continued, “Because it is a timeshare in a facility that can apply standard industry tools at an economy of scale that an individual person can’t. We need to have that conversation if we think about cybersecurity and facilitating interoperability.”

SECURING MORE INFORMATION

It’s important to stay up-to-date on security threats and effective innovations to fight them. Recommended sources for more information include:

[Healthcare IT News](www.healthcareitnews.com)  [Hacker News](www.thehackernews.com)  [Security Week](www.securityweek.com)

For physicians and practice administrators with limited IT experience and time, unloading a majority of the data security vigilance to a qualified cloud-based vendor can be an effective strategy.

We hope this report helps you make an educated decision on how to fortify the security of the data stored by your medical group. We take data security very seriously at CareCloud. We use Akamai, Amazon Web Services and Verizon Terremark as part of a comprehensive approach to secure data. These protections are included in the per-provider monthly pricing of our meaningful use certified EHR and cloud-based practice management systems.

To learn more about how CareCloud’s software and services can help your medical organization run more efficiently, securely and profitably, visit CareCloud.com or call 1-877-342-7519.
References:


9) Google: Creating a strong password: https://support.google.com/accounts/answer/32040?hl=en


