The Conscience of EMS JEMS JOURNAL OF EMERGENCY MEDICAL SERVICES

SECURE IN THE Cloud

THE NEW PUBLIC VS. PRIVATE DEBATE IS IN DATA SECURITY

›› BY TODD STOUT

If you have a smartphone, chances are some of your information and data is stored in "the cloud." If you use e-mail from Google, Yahoo, AOL or Apple, you're using "the cloud." If you're on Facebook, LinkedIn, Twitter, Google-Plus or other social media, you've got data in "the cloud."

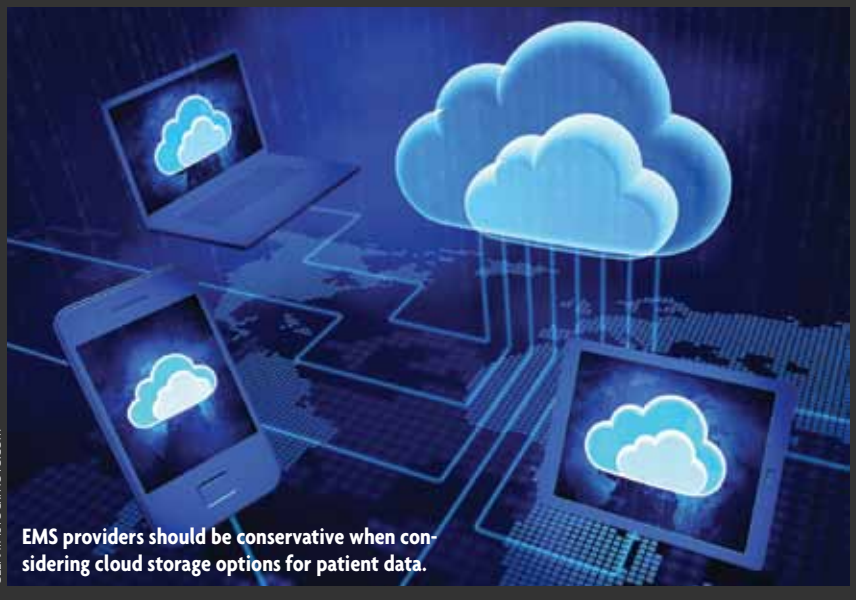
You might wonder what the cloud is all about. In actuality, there isn't really one "cloud," but rather many small and large networks of servers owned and managed by technology companies. Although experts debate many definitions, the main thing most EMS providers need to know is that software and data stored in the cloud is stored on computers and hard drives somewhere else, and that someone else owns and manages them. The computers may or may not be in the same city, the same state or even the same country as you. In fact, the software or data may not be in only one physical location or even in one country, but it may be spread apart geographically with different components of the program or pieces of data located on servers thousands of miles apart.

PRIVATE VS. PUBLIC

Private clouds are usually application- and vendor-specific, such as cloud-based storage provider DropBox and Apple's iCloud. In EMS, the most common examples of private clouds are the various hosted electronic patient care records (ePCR) systems, like those offered by EMS Charts, ESO, HealthEMS, ImageTrend, TriTech and ZOLL. In the hosted versions of these systems, the data used by the application is stored on remote servers and accessed via the Internet. Other EMS private cloud examples include online education provider CentreLearn and my own real-time data intelligence and dashboard provider, FirstWatch.

Public clouds are typically larger, commercially available sets of servers where developers can basically rent space. Some of the best-known examples are Google Cloud and Amazon Web Services. In the future, we'll see more software developers using these and similar public clouds as the foundation and infrastructure for their systems. They can offer advantages for developers, and even end-users, but EMS providers need to think carefully about what data they allow to be stored in public clouds.

As healthcare providers, EMS agencies need to protect patient privacy, and the Health Insurance Portability and Accountability Act (HIPAA) provides the guidance and sets the rules that help ensure patient privacy. HIPAA's technical details and complex rules can be confusing, and they were developed prior to the evolution of the cloud, so it's not exactly clear how these rules relate to the cloud. However, it's only a matter of time before the federal government clarifies if and how the public cloud can be used to store patient medical data. Until then, I'd advise agencies to stick with storing data locally or in HIPAA-compliant private cloud servers that are owned and managed by companies you know and trust.



EMS providers should be conservative when considering cloud storage options for patient data.

OLENAT/ISTOCKPHOTO.COM

HUMAN & OTHER RISK FACTORS

Recently, some public stories of security breaches and data theft at large cloud providers or customers have come out regarding DropBox, Google and NASDAQ. Although hardcore hackers get the most publicity for their role in these crimes, the reality is that in most computer, network and cloud security breaches, staff and customers are the weakest links. This large group of users can unknowingly compromise security in a number of ways. These include social engineering scams, where hackers convince someone to reveal login information, as well as leaving a laptop where it can be stolen or improperly securing backups. Other times, the entry point to a network is due to people using the same login and password on multiple systems. This means that once one system is breached or hacked, it often leaves the door wide open for hackers to gain entry to other systems.

For example, some people use the same login credentals for many websites. If they use that to log on to external websites, such as Gmail, Dropbox or Yahoo, and a hacker gets access to their username and password information on one of those sites, then the hacker also has the username and password for every other site the person uses, including hosted EMS systems.

When deciding whether to use a hosted or cloud-based vendor, think of it this way: If you have your own servers and employ the staff to manage them, your human risk is limited to your own staff. If you choose to use applications on private or public clouds, your human risk includes their staff and potentially their other customers. Larger cloud providers have more servers, which require more people to manage them. This increases your risk.

Additionally, some of those providers have servers in different countries, which likely have different standards and could have less oversight. And, because of the Internet and an increasingly global economy, those providers may not be based in the same country you are. But it's often hard to tell that from their marketing materials.

Of course, human error isn't the only cause of security problems. Others include physical security and hardware, software setup of the servers and network, the way the software is written and the way the data is stored. All of those factors need to be considered when choosing a cloud provider. It's complex and difficult to evaluate, even for information technology professionals.

Many reputable software companies contract with outside computer security services to audit their security, and they're proud to let you know that. I've also seen external auditing as a requirement in requests for proposals for cloud services. This is smart because you can have tested and audited website and web application security just like you can have audited financial statements. Although it's not a guarantee that your data is secure, it's a step in the right direction.

RECOMMENDATIONS

It's fairly common to use hosted applications (or private clouds) in EMS for all kinds of HIPAA-regulated data, as well as other private and public data. Depending on the needs of your agency, this can make good sense for your organization. But do your homework to make sure you know where your data is going and that it's secure there, preferably by trusted third-party security audits.

I would suggest only using public cloud applications for data that is not critical to keep private, such as clinical protocols, disaster procedures or marketing materials, as well as in instances where your data needs to be readily available and accessible. And although I think public cloud security will get better, for now I'd be wary of solutions that store private or HIPAA-regulated data in public clouds because the potential risk is very high. JEMS

Todd Stout is president of FirstWatch Solutions Inc. He started his EMS career as an ambulance stock boy in Kansas City over 30 years ago, and has worked as an EMT, paramedic, flight medic, and EMS manager for public and private providers before moving into the software side of public safety. He is a National EMS Management Association (NEMSMA) Board member and was named one of the top 10 innovators in EMS by in 2011. He can be reached at tstout@firstwatch.net.

The Conscience of EMS
JEMS
JOURNAL OF EMERGENCY MEDICAL SERVICES

Reprinted with permission from the
December 2012 edition of JEMS,
Journal of Emergency Medical Services.