With cloud computing, sorting out pros, cons

Anne Paxton

April 2017—"No man putteth new wine into old wineskins" reads the biblical aphorism in Luke 5:36–39, which continues by giving the reason: "The new wine would burst the skins and be spilled, and the skins would perish." Old wineskins, biblical scholars say, would typically be stretched to the limit or become brittle as wine had fermented in them.

On the subject of cloud computing versus local servers, one's first thoughts might not relate to wineskins. But as ever more data storage and applications migrate to the Internet, the idea of data that might spill and databases that might burst by becoming unsecure—not to mention files that might perish—does resonate in the hospital world.

Across health care, cloud computing—or computing on demand via the Internet—has become pervasive. Its initial appeal has often been the huge capacity of outside data storage through file-sharing services that now include Dropbox, Google Drive, Microsoft OneDrive, or Apple iCloud. But software as a service that no longer has to be locally installed is swiftly becoming an even more important part of cloud computing.

The National Institute of Standards and Technology defines cloud service as a "pool" of configurable computing resources—networks, servers, storage, software, services—where the user generally has no control over or knowledge of the exact location of the provided services. This pool of resources is accessible by a variety of platforms and is tapped into, often automatically, based on user demand.

The primary advantage of using cloud servers is the ability to get storage and processing power as needed, which is helpful for large sets of data and cost-efficient for users, who can be charged on a pay-per-use model.

Dr. Tuthill

"To a certain extent, we have had what you might call 'enterprise computing' within hospital organizations for at least two decades, because we've had shared storage drives and shared back-end storage systems," says J. Mark Tuthill, MD, division head of pathology informatics, Henry Ford Health System. But now, systems like Microsoft Active Directory or Citrix connect hospitals to many software packages and allow them to run multiple heavily used applications. Epic's electronic health record is served through a Citrix interface, while Cerner offers a type of installation of its electronic medical record as a software service, Dr. Tuthill points out. "So you may not be installing Cerner in your data center or your hospital; you're actually getting a secure instance of Cerner that they host in the cloud."

"You can see how gray some of this can be," he says. "But cloud computing is really just an Internet-enabled extension of enterprise computing, which is possible due to the low cost of storage as well as the markedly increased bandwidth that we have on the Internet now." In fact, people use the cloud, often unknowingly, when they access anything through their browser, because the cloud is based on Internet technology.

In the past, services like file transfer protocol or secure file transfer protocol might typically be used to move large data files around. "Now we actually use business cloud services to do secure exchange of data." Henry Ford also

uses a couple of different apps to securely upload data into the cloud to companies that perform data analysis and return the data.

Dr. Tuthill's health system has pre-credentialed cloud storage service providers to use for potential business apps by putting them through a rigorous security review, including third-party audits and a rigorous contracting process.

In molecular diagnostics, companies can use "secure Internet connectivity"—i.e. cloud computing—that allows analytics on molecular files, Dr. Tuthill says. For example, clients can upload their genetic sequences to Agilent, which will process them and return a report.

He doesn't see this practice as standard yet. "I would say it's an option or an opportunity, in many places. The large academic centers particularly are doing this in a very sophisticated way. They have their own internal network setup so they are really using internal enterprise computing."

Smaller community hospitals could benefit the most from cloud services, Dr. Tuthill says. "If you don't have the data center for storage and don't want to hire all the people and do all the maintenance, you may want to use the cloud ahead of large institutions with massive infrastructures and much larger data needs. Some of their apps require storing tens of terabytes of data, and that's not something you're going to buy cheap right now on the cloud." So he thinks smaller hospitals may be earlier adopters of cloud computing than the larger academic hospitals.

There is also the concept of a "private cloud."

"This is software that uses Internet service but that is privatized by the way data storage is set up and how you're secured," he says. Henry Ford has such a storage system and considers it secure. "The rest of the world can't get in here; it's behind our firewall." The key component to a private cloud is the use of "thin client" and Internet web services to carry out the communications, he says.

For next-generation sequencing data, there is no getting around it: The cloud environment is becoming essential. "One of the reasons for that is the volume of the data that needs to be analyzed and potentially the collaboration of those data sets," Dr. Tuthill says. "In molecular diagnostics, particularly in research, you have to have a large data set, and typically that's not going to be within one organization so people have to collaborate."

Cloud computing has a direct relationship with what is called "grid computing."

"Grid computing actually leverages the power of hundreds of thousands of computers to do analysis as opposed to a single desktop or single server or even a set of servers in your organization. And this allows you to achieve things like 'big data' computations." As one example, NASA has set up cloud programs in which people can volunteer their computers at night while they're asleep, allowing the computers to help NASA solve astrophysics problems.

"Cancer analysis and genome sequencing analysis could leverage this type of technology as well," Dr. Tuthill notes. "Having 10,000 computers all working on a problem together is obviously strong computational power."

Some relatively small LIS vendors have started to provide LIS services from the cloud, but the large companies, except for Cerner, still use the classic client-server model, Dr. Tuthill says. One reason is that tying into physical devices like instruments and printers is more difficult in cloud environments. But he thinks the pattern will change in 10 or 15 years. "You will likely see most people running their labs hosted in a data center with shared resources. That's largely because of the huge maintenance cost. If your LIS vendor is going to update your LIS and they can do that in one place, versus on five different servers, making them touch all your workstations, you have eliminated a tremendous amount of maintenance."

Cloud computing can also help laboratories automate their workflow or improve other lab processes, depending on how the software is built. "I think it can really get down to the level of interfacing instruments into it. You're going to see a lot more vendors take their platforms into cloud services with 'software as a service.' If you look at other industries, you're just seeing this in spades from people who offer customer relationship management tools that

are hosted solutions. Our outreach portal is really 'software as a service'; it uses cloud technology to help us service our outreach customers."

Fears about security may or may not be overblown, Dr. Tuthill says. "On the one hand, if you are using the cloud to store things and it's fully secure, and your company follows best practices, you've got a wrapper around your data. It's better than using notebooks or thumb drives, which get lost, and you end up in the newspaper for HIPAA violations. So a network securing your data, and providing people access to it through cloud computing technology, has inherent advantages." The ability of companies like Amazon and IBM to back up their data and ensure there are no viruses is inherently more maintainable and less expensive than what hospitals may have in their data centers, he adds.

But an inherent risk of using cloud services is that you may expose yourself to malfeasance on the part of the employees of the cloud company. "If you have a bad actor who decides they want to screw up your health system, they could do something to hack you or break you. Frankly, those are risks we face inside our own organization as well. But it does start to require a lot more effort in terms of security review when you step outside your firewalls."

When vetting a company, Dr. Tuthill always asks if they have had their facility reviewed by a security analysis firm, and how they get assurances about their employees' reliability. "The large cloud services, most of them, have ensured that data is encrypted to nonusers of the information. But somebody can always break through the security glass if you become complacent."

Reducing capital investment in information technology is a clear advantage of the cloud, Dr. Tuthill says. On the flip side, there are privacy and security issues to take into account. "The patient doesn't usually ask us, 'Where are your records hosted?' And we don't ask, 'Do you mind if we store your data in our data center?' It's just not a big part of the conversation."

For most such questions, HIPAA privacy regulations step in as the patient's proxy. "And the HIPAA rules have gotten a lot more stringent as of 2013. We have had to recertify all of our vendors for the new HIPAA rules, but that's partly driven by the desire to protect the patient's interest." Meanwhile, ironically, patients surf to online health charts on Amazon and Google and blithely fill in the blanks. "Some patients have no compunction about putting all of their information into a cloud program like that; others may not."

Some diagnostic disorders like HIV or unique genetic diseases pose a special risk, Dr. Tuthill says, if a patient could be identified, though he's never seen such a thing happen. "That said, we're very careful. We have our patient portal, which we're required to provide by the HITECH Act, so patients can view their lab results, schedule appointments, and communicate with their doctor, and we have excluded some lab results such as HIV and sexually transmitted disease results from going into that portal."

Until recently, all anatomic pathology results were also excluded from the patient portal at Henry Ford. "This was because we did not want to have patients' first notice of a cancer diagnosis in the form of a message in their portal. But we have reversed course on that and are taking a less paternalistic approach. We basically say the doctor should be in touch with the patient and release the diagnosis within three days. This was driven in part by patients' requests as much as law."

In short, he views less expense and greater security as the basic benefits of the cloud. "If you just look at the consumer model, if you can get a terabyte of storage from Amazon Web Services for $250 a year, it may sound expensive. But it's not expensive when the hard drive at home crashes and you've just lost a collection of family pictures from the last 15 years. I do think the cloud will be a much more cost-effective approach for everybody, not just industry, and not just in health care."

Physician informaticist Alexis B. Carter, MD, on the other hand, is far less sanguine about cloud computing. While cloud services have distinct advantages, laboratory directors should know that the security and privacy risks

are substantial, and every available form of mitigating those risks has limits, she says. For her, these downsides are a deal-breaker. “I don’t use the cloud if I can possibly avoid it,” says Dr. Carter, of the Department of Pathology and Laboratory Medicine at Children’s Healthcare of Atlanta.

Dr. Carter

Her major concern is the requirements of the HIPAA Privacy Rule, in effect since 2003, and the HIPAA Security Rule, which took effect in 2005. These rules protect all health information that can be linked to a unique individual, and set administrative, physical, and technical safeguards for personal health information stored or used on any electronic media. Since 2009, the HITECH law has imposed stiff penalties for noncompliance with HIPAA, particularly where there are security breaches compromising data, and the HIPAA Omnibus Rule has required that genetic information (as defined under the Genetic Information Nondiscrimination Act) be treated as protected health information under HIPAA.

As health entities confront escalating health data security breaches, this collection of federal laws has enormous implications for data in the cloud, Dr. Carter says. She has looked at cloud servers and finds that the ones that are even somewhat secure under HIPAA are inordinately expensive. “Hospitals that say they’re using a HIPAA-compliant cloud may not realize that it’s only covering one of the three different categories of safeguards under the HIPAA final security rule.”

In addition to the security issues, putting records on the cloud also potentially eliminates the laboratory’s ability to directly integrate data within its EHR or LIS. In her experience, EHRs and LISs are proprietary and tend only to engage in HL7 real-time interfaces with other known instruments and platforms, not with the cloud.

Laboratories that turn to the cloud to save patient files generated from their next-generation sequencing instrument do acquire a lot more computing power, allowing faster processing than would be possible in-house, Dr. Carter says. “It means you’re not going to have to hire three FTEs. But I happen to know that a number of places are not using the HIPAA version of the cloud, thinking that if they remove the patient name and date of birth and apply an identifier number, but leave the sequence intact, they’re going to be okay with the law. And that’s not what I understand that the law requires.” In fact, she notes, there have been researchers who have published their ability to go back and re-identify individuals just based on their sequence.

The second issue is that people may falsely believe the cloud is secure and nobody can get to their data. “That’s not the case—not unless they have paid extra money and put in additional pieces of software to help monitor and audit who has access to the data.” She does not believe security breakdowns are inevitable, “but data breaches are doing nothing but getting worse.”

Unfortunately, people are buying into cloud services without full knowledge of these risks, in some cases preferring not to know because it will be more difficult and costly. But deciding to ignore the regulations can be considered willful neglect, from the viewpoint of the Department of Health and Human Services’ Office for Civil Rights. “Some institutions are running on the expectation they are not going to get caught. But if they do get caught, especially for breaches and willful neglect involving over 500 patients, I have seen the fines be in the $1 million or greater range.”

Laboratories that are considering cloud services should make sure they consult someone knowledgeable about the cloud and how to use it, to make sure it’s a feasible, secure, and cost-effective option, given all the safeguards needed. “You may have to hire someone and that’s going to add costs, but if you can’t hire someone, I wouldn’t do

it."

Virtual servers are somewhat different from the cloud, Dr. Carter notes. "The cloud means you are using servers in a location where you have no idea where they are and the company hosting your software may move it from one storage place to another without your knowing. With a virtual server, you typically know exactly what data center your data are sitting in. For example, Cerner has a huge data center in Kansas City where they remotely host a bunch of EMRs as well as LISs."

In such a virtual server remotely hosted system, the risks are a lot lower because "you have more control over the systems and software, so you can ensure that all the HIPAA safeguards are built in." With the cloud, on the other hand, she says, "The biggest issue for me is security. The vendor providing cloud services has an insane level of control over how secure it's going to be, and sometimes you really have to dig to find out where the holes might be in how they've set things up." Some cloud providers have even attempted to hold people's data hostage as security for payment, Dr. Carter notes, but the Office for Civil Rights has been clear that no cloud provider can hold on to patient data. "They're required to hand it back over and then securely delete whatever is left on their servers."

In addition to those risks, many people may not realize that HIPAA requires a BAA (business associate agreement) document if there is any personal health information—even a de-identified genome sequence—on the cloud. "We've had NGS providers who have refused to sign a BAA because it basically makes the vendor be compliant with HIPAA and liable for theft, loss, or lack of security of the data." But if labs are using the cloud and don't have a BAA, they can be subject to fines by HHS. "Every year the Office for Civil Rights puts out how much money they make in fines from auditing people who are not compliant with HIPAA, and since 2003 there have been close to $50 million in fines."

She suspects there is a lot of noncompliance and cautions that institutions have more to worry about than fines. Multiple institutions have had data go missing for large numbers of patients. "Even when no one could determine any evidence of wrongdoing, the breach notification rule under HITECH required that these institutions shell out millions of dollars per data loss to hire a public relations firm, contact patients, and offer them security monitoring for a year. And all this was without the Office for Civil Rights coming in and deciding to audit them."

Nevertheless, the cloud continues to grow because typical NGS workflows and pipelines—algorithms that can be run in parallel to convert data—require quite a bit of computational power, Dr. Carter points out. "NGS is not the same as having a lab instrument and putting samples on it. There is a huge amount of validation that takes place. And if you decide you do not want to buy servers and have them sitting in your lab and instead want someone else to manage the servers, that's often a reason why people—particularly at academic medical centers and large commercial laboratories—would want to use the cloud." Cloud services are also often able to use hundreds of processors at one time, which can reduce NGS computational time, she notes.

Not every expert agrees that cloud computing represents a revolution. At one time, moving computing to local servers was considered an advance because of the unreliability of data communication, says Raymond D. Aller, MD, emeritus professor of pathology and former director of pathology informatics at the University of Southern California. And some hospitals, for many years, vowed to never take their files to the anything-goes environment of the Internet. "But now we have much faster, much more reliable, and redundant communication where there are multiple paths to get from the laboratory to a central server area, and servers may be distributed over data centers in several states, so if there's a disaster, there is backup."

Dr. Aller agrees that the security risks of having your server resources somewhere else are substantial. "Laboratory data needs, for medical reasons and social reasons, to be kept confidential. If a hacker got a list of all patients with HIV or sexually transmitted disease, there are many lab tests we really don't want our neighbors to know about. Or results could be used as a substrate for blackmail, say through a threat to give data to a local newspaper and cause damage to a hospital." In terms of the overall cloud architecture, he adds, that's one of the

biggest risks and concerns.

For laboratory workflow, Dr. Aller is skeptical of the benefits of cloud computing. “Automating workflow depends on how much you can rely on the speed and reliability of your network. If you have a robotic system running specimens throughout your lab, I suspect you’ll want a local controller for that because the timing between robots and instruments is critical; you don’t want intermittency in your response time. Maybe the central computer does the billing, but probably not workflow.”

The vaunted economies of the cloud may not materialize for the laboratory, he believes. “Vendors will say to use the cloud because you don’t have to have your own servers, which require work to buy and maintain, and to upgrade you have to buy a whole new set. But depending on how much they charge for the use of their servers, there may or may not be an economic advantage to using the cloud.”

Not long ago, he recalls, at one large data center maintained in the Midwest, which had 200 hospitals running on it, an engineer in the data center made a mistake setting up some control software. “That mistake propagated, so half of the hospitals in the network were down for several hours. So that’s a risk if you’ve got a single mass of software and databases.”

Sometimes hospitals can end up with even less functionality too. In another case he recalls, a four-hospital system serving millions of patients chose an EMR that was cloud based over another vendor’s product because the health care facility would not have to maintain its own servers and databases. But when the hospital wanted to add a test or a couple of elements to a patient report, it had to go through a central administration at a remote location. “What this hospital system ended up with was basically rigid control from thousands of miles away, and they did not have the flexibility to serve their own patients.”

Centralizing all of a hospital’s resources with a megadata center also carries risk, he notes, pointing to a recent instance of Amazon’s servers being down for several hours. In such a case, he says, you just have a larger single point of failure, and that’s contrary to the ideal of the Internet, which is to distribute risk. “If you have a single point of failure, it doesn’t matter if it’s in your own data center or back in Minneapolis, if you are connected to resources that aren’t helping.”

Next-generation sequencing may or may not thrive from storage in the cloud. “NGS and other kinds of genetic tools do have petabytes of data. It’s more challenging to push that data across the Internet, which has only a certain bandwidth, so it may not be the ideal approach. On the other hand, on the cloud it may be cheaper to buy that storage and there may be providers that will provide you the computers to crunch that data. When you have a map of genetic data, you need a place to put it, a way of crunching it, and a way to display it. You need specialized software, and if you’re Memorial Sloan Kettering, you can do it all in your lab. But for others, bringing all that ‘capacity to crunch’ down in to a local lab may be less practical than it used to be.”

Still, in Dr. Aller’s view, some companies may be overpromising when it comes to cloud computing. “Somehow cloud computing was going to be the solution to all bugs, capacity, and software problems.” But that’s not true, and, he adds, risks such as ransomware (where hackers encrypt a company’s data and promise the decryption code only if a ransom is paid) have been on the increase. “A few years ago, hospitals said we’re not going to connect our hospital network to the Internet, but you can’t get away with that now; you have to connect your systems to the Internet. And when you do that, there are people in various countries who have found a way to lock up your files and demand a ransom for you to have access again.”

Dr. Tuthill, for his part, doesn’t believe the cloud increases hospitals’ exposure to ransomware. He sees room for debate about the kind of security risks that cloud services can open up. “I think most of these organizations that have had their data taken and held for ransom have had lax security practices, and because their data is local, it’s much easier for them to ransom a hospital. It would be much more difficult to do with a cloud service that was using best practices in a large industrial setting.” However, he adds, the arguments about cloud computing cut both ways. “You could probably have an hour-long conversation over a glass of wine and still come out of it saying, ‘Well, I’m not sure.’” So debate continues, but hospitals’ use of cloud services is probably here to stay.n

[hr]

Anne Paxton is a writer and attorney in Seattle.