Cloud computing provides access to a variety of IT resources wherever and whenever needed, including processing capacity, software, infrastructure and development tools that are hosted either by a third party or internally and delivered as a service.

In healthcare, cloud computing can support a wide range of organizational structures and business services, such as electronic health records, e-prescribing, practice management, computerized physician order entry (CPOE), billing and administration, etc.

Cloud computing offers a new and flexible model for deploying technology. “Clouds” let healthcare organizations expand or contract resources as needs dictate, thereby allowing them to pay only for what is needed at any given time.

The economies, scalability, and deployment capabilities afforded by cloud computing offer a compelling return on investment, an increased ease of ownership and better support of organizational processing needs.

The healthcare industry has not rushed to the cloud as quickly as many other industries, but a fast-growing number of healthcare cloud-based services are available, and certainly interest is growing among healthcare providers.

Small entities tend to be lean on IT support and can benefit from leveraging cloud provider investments in infrastructure. Hospitals and larger health systems can benefit from cloud solutions that adapt immediately to changes in demand for the amount of IT processing required, along with reduced need for capital investments in IT and more rapid deployment of technology.

Cloud technologies are particularly attractive as health systems rush to qualify for more than $20 billion in U.S. government financial incentives under the Health Information Technology for Economic and Clinical Health (HITECH) Act by meeting deadlines for the Meaningful Use of certified Electronic Health Record (EHR) technology. Small and large providers are finding that cloud-based EHRs can be implemented quickly and cost-effectively.

Understanding the cloud
Each of multiple types of cloud computing architecture can meet differing IT needs. The type of architecture used will determine the location and possession of the hosted applications and data. The three main types of cloud architecture are:

- **External/public – Shared computing** resources maintained by an off-site third-party provider that offers pay-per-use access to data, applications, infrastructure, etc.
- **Internal/private – Dedicated** computer resources provided by an offsite third-party, or use of cloud technologies on a private internal network that is managed and maintained by in-house IT staff
- **Hybrid – Multiple mixed-use public/private clouds**, integrating on-site IT cloud infrastructure with third-party provider services

In addition to architectural differences, there are also five main types of service delivery that may be offered through cloud technology:

- **Infrastructure as a Service (IaaS)** – Remote computer infrastructure delivery; for example, access to servers, software, voice-over-Internet-protocol (VOIP) and networking, which could be particularly useful for smaller providers with limited resources
- **Platform as a Service (PaaS)** – Full or partial operating-system/development-environment delivery that supports online access and collaboration and provides access to a robust toolset
- **Software as a Service (SaaS)** – Software applications delivery, eliminating the need for in-house development or hosting, such as a web-based EHR or radiology information system (RIS)
- **Desktop as a Service (DaaS)** – Provides remote access to an individual workstation and its operating system and storage hardware
- **Business Process as a Service (BPaaS)** – Similar to SaaS, but rather than hosting applications, the cloud provider hosts specific business processes (such as benefits management, help desk support or procurement) for multiple internal or external customers

**Potential advantages**
Cloud computing offers a number of distinct advantages for healthcare
providers, including efficient and cost-effective use of internal resources, greater speed to deployment, lower operating and capital costs and higher performance.

Because the use of cloud technology results in the dynamic allocation of resources as needed, organizations can move away from the old model of having to make upfront capital IT investments beyond current needs in order to provide for future capacity requirements. Dynamic de-provisioning releases resources back into a common pool for reallocation to others as needed.

### Determining the Organization's Use of Cloud Services

Cloud structures also allow for a more rapid deployment of infrastructure, applications and upgrades as they can be distributed via a network vs. having to go “desk to desk.” With less physical infrastructure, organizations can save on personnel, facility, energy and maintenance costs, and can align spending with organizational needs. Cloud models are also highly scalable, providing the ability to support either growth or peak-use needs, and serve to enhance the interoperability of disparate hardware components and software applications.

### Managing Cloud Risks

Along with the significant advantages it offers, the cloud also presents a new set of risks that must be managed. From an internal audit perspective, these risks can be divided into six key areas:

- Data security and controls
- Regulatory compliance
- Multi-tenancy
- Location
- Reliability
- Sustainability

Anticipating the impact on and influence of the internal and external audit function is crucial when preparing for cloud computing implementation, managing cloud risks going forward, ensuring proper alignment of hosted service contracts and seeing that organizational financial data and personally identifiable information (PII) is adequately secured.

### Data Security and Controls

- The cloud provider’s security policies and internal controls may not be as strong as the organization’s. Third-party reliance is compounded by the exposure of data that must now be transmitted via the Internet.

Internal audit should determine if the cloud provider has a Statement on Standards for Attestation Engagements No. 16 (SSAE 16 – formerly SAS 70) that addresses their control environment. Some vendors may have SSAE 16 evaluations that do not adequately address each of internal audit’s control concerns, and some may not have had the assessment performed at all.

If the provider has not undergone an SSAE 16 review, ensure that the provider contract allows for on-site security audits on request (i.e., a “right to audit” clause). Also, verify that minimum control standards are clearly defined in the vendor Service Level Agreement (SLA).

Internal audit should determine if the cloud provider’s security posture is based on a security standard (e.g., ISO27001, Cloud Security Alliance, PCI DSS, etc.) and if the cloud provider has had a security assessment performed.

### Regulatory Compliance

- The organization depends on the provider’s knowledge of and conformity to industry-specific compliance requirements, legal standards, and foreign business or national laws/regulations based on where data is stored.

Compliance standards that apply to most healthcare institutions include the Health Insurance Portability and Accountability Act (HIPAA) and HITECH, among others. Internal audit will need to revisit any prior analysis conducted regarding HIPAA compliance if the organization elects to move to a cloud platform.

Institutions must consider state privacy or security laws, such as Massachusetts’ data protection law and California’s data breach notification law.

If hosted data is stored in international locations, healthcare organizations must verify that compliance is maintained with applicable countries’ business laws/regulations. This can apply even if data is only stored internationally as backup. Internal audit must be sure to identify all data storage and cloud processing physical locations, research all applicable rules, and determine the vendor’s approach and degree of compliance.

In most industries, the legal responsibility to meet a regulation falls fully on the organization, not necessarily the vendor. In healthcare, per HIPAA, the vendor may be considered a “covered entity” under the
Moving to the cloud

The decision to use cloud technology is fundamentally a business outsourcing decision rather than a technology decision. Before moving some—or all—of their computer processing into the cloud, healthcare organizations must consider a number of factors. 

Organization decision-makers need to weigh how comfortable they are with entering into a partnering arrangement with a third party, and internal audit has a key role to play in this evaluation. They should duly consider everything from a potential provider’s financial strength, to its reputational integrity, to the levels of service it provides, to the organization’s ability to withdraw from the relationship if necessary. 

After that, internal audit must address how well-constructed the provider’s operational and technology controls are with respect to:

- Confidentiality
- Privacy
- Availability
- Security
- Compliance

Pay particular attention to the range of healthcare regulations, including HIPAA and HITECH. An evaluation of services provided should take into account the standardization that accompanies third-party offerings versus the customized fit of in-house solutions.

Only after all these issues have been addressed do technology concerns come to the fore; cloud technologies should be aligned with the organization’s short- and long-term IT and business strategies.

Cloud computing represents the next step in the evolution of healthcare technology and promises to transform healthcare organizations’ IT deployment. The question is not whether healthcare organizations will adopt it, but when and how. If they perform the right due diligence with active engagement by internal audit, they will find success in embracing cloud computing.

Mark T. Oster is the Partner-in-Charge, National Not-for-Profit Business Advisory Services Practice. Mark is the Business Advisory Services principal responsible for providing business strategy, operations improvement, information technology and business risk services to Grant Thornton’s not-for-profit clients. You can reach Mark by telephone at (212) 542-9770 or by email at Mark.Oster@gt.com.