FOLEY

FOLEY & LARDNER LLP

Prepared by Foley's Health Care Industry Team and
IT & Outsourcing Practice

Cloud Computing for Health Care Organizations

October 2012

FOLEY
FOLEY & LARDNER LLP

Cloud Computing for Health Care Organizations — A Practical Framework for Managing Risks

Cloud computing is no longer a new trend; it is a standard approach to the management of information technology (IT) resources. According to Gartner Group, cloud computing is expected to represent a $150 billion market by 2014.[1] In a 2011 cloud computing tracking poll, 84 percent of all IT professionals surveyed said that their organization has already employed at least one cloud application, and 30 percent of those in health care organizations reported implementation or usage of cloud computing.[2]

Although other business sectors may be leading the way, the health care industry's adoption of cloud computing is rapidly accelerating. Spurred in part by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which provides federal incentives for the meaningful use of certified electronic health record (EHR) technology,[3] health care providers are rapidly modernizing their IT infrastructure and outsourcing data storage and transmission. Growing numbers of vendors are offering services such as electronic medical records, medical imaging, telemedicine, and care management that can be used by health care providers, payers, and patients over a cloud, providing health care organizations with an array of options to manage their IT needs.[4] Because of the lower cost, reduced investment in IT infrastructure, increased resource availability, and ability to rapidly deploy health IT, cloud computing is becoming an increasingly attractive option for health care organizations.

However, cloud computing is not without substantial risk, particularly at a time when health care organizations are finding themselves subject to myriad state and federal data security and privacy laws. When an organization's most sensitive data is hosted by a cloud provider, it is subject to the additional security risks associated with the cloud computing environment. At a time of heightened enforcement of privacy and security laws and increasing penalties associated with failure to adequately protect sensitive data, relinquishing control of key organizational assets to a cloud provider — even one with that meets high standards — requires a high measure of confidence.

Moreover, because the electronic privacy laws have failed to keep pace with advances in technology, there is limited regulatory oversight of cloud computing providers. Industry efforts led by organizations such as the Cloud Security Alliance and the National Institute for Standards and Technology have established best practices for security in cloud computing,[5] but these efforts fall far short of legal protection. This has led Foley, working together with our clients, to develop the contractual framework provided in this white paper for risk management and mitigation for outsourcing health care data to a cloud environment.

What Is Cloud Computing?

There have been many different definitions for the term "cloud computing" proposed by technology experts and a wide range of organizations, including service providers, IT research firms, government agencies, and educational institutions. Several popular definitions are provided in Appendix A (Definitions).

The different definitions and lack of agreement around a single definition have created confusion as to what cloud computing really means. Many of the proposed cloud computing definitions have been criticized as being too broad and vague, which has allowed the term to be applied to almost any technology developed today and leading many to view cloud computing as simply a new marketing term to describe existing service delivery models. For purposes of this white paper, we attribute the following high-level characteristics to a cloud computing service delivery model: (i) delivery over the Internet (cloud), (ii) software, platform, or infrastructure resources provided as services, (iii) scalability on-demand, and (iv) utility and/or subscription billing (i.e., payment based on the customer's actual use and/or a period of time). There are three well-known service delivery models for cloud computing: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Appendix B (Cloud Computing Features and Comparison) provides additional descriptions of common features of cloud computing, and compares a cloud computing SaaS to some existing delivery models, specifically the Application Service Provider (ASP).

A cloud computing approach to IT services can offer many benefits, including cost reduction and service flexibility. By moving software and infrastructure to the provider's remote data center, customers (such as health care organizations) may be able to lower some of the up-front risk and complexity associated with realizing the benefits of new technology. Customers may achieve a reduction in capital costs, including the up-front investment in new infrastructure, new software licenses, and personnel hiring and/or training. In addition, less equipment means that less physical space at a customer site is needed to store such devices. Further, there may be lower costs as a result of reductions in planning, purchasing, installing, maintaining, managing, and supporting the software and infrastructure, and hiring, training, and managing an IT staff.

In addition, customers are attracted to the flexibility of being able to (i) quickly set up and implement an IT solution, (ii) access services from anywhere, at any time via the Internet, and (iii) quickly add and remove IT resources on-demand, so that customers can effectively respond to the growing push for IT adoption and modernization. Despite these benefits, health care organizations must protect against a non-disciplined rush to cloud computing. The risks associated with the usage of a cloud provider to support a critical business process or to host sensitive health data can outweigh these benefits.

What Are the Various Models of Deployment for Cloud Computing?

There are various models of deployment for cloud computing, including public, private, community, and hybrid clouds. A public cloud is one that is owned and operated by a cloud provider delivering cloud services to its customers (including health care organizations) in general and, by definition, is external to the customer's organization. The infrastructure and the computational resources are made available over the Internet. At the other end of the spectrum are private clouds. A private cloud is one in which the computing environment is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization's data center or outside of it. A private cloud has the potential to give the organization greater control over the infrastructure, computational resources, and cloud customers than can a public cloud.

Two other deployment models exist: community and hybrid clouds. A community cloud falls between public and private cloud. It is somewhat similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization. Hybrid clouds are more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public).

Each member remains a unique entity, but is bound to the others through standardized or proprietary technology that enables application and data portability among them.[6]

While the choice of deployment model has implications for the security and privacy of a system, the deployment model itself does not dictate the level of security and privacy of specific cloud offerings. Unless the customer is a large enterprise that contracts for a private cloud solution, the cloud computing environment, technologies, and approaches used to facilitate scalability, such as virtualization and multi-tenancy, may result in customer data being stored on a physical server that also stores data of the provider's other customers (i.e., the physical server is divided into two or more "virtual" machines or servers). The multi-tenant environment may increase the risk of unauthorized disclosure, but ultimately, the level of security and privacy is dependent on the strength of the security and privacy controls, the financial and operational soundness of the cloud provider, and the extent of visibility into performance and management details of the cloud environment.

What Are the Challenges for Health Care Organizations Considering Cloud Computing?

Assuring the cloud provider's compliance with the privacy and security requirements imposed on health care organizations is a significant challenge. Health care is a highly regulated industry, and the data used and maintained by health care organizations is subject to a plethora of federal and state laws that govern individually identifiable health information, employee data, credit card data, and other sensitive information. Although these laws establish certain common privacy security safeguards, they also impose discrete requirements, resulting in legal standards that are generally consistent but dissimilar with respect to the particulars.

Health plans, health care clearinghouses, and covered health care providers (i.e., covered entities) are required to safeguard Protected Health Information (PHI) by the Health and Insurance Portability and Accountability Act of 1996 (HIPAA)[7] as modified by the HITECH Act and their implementing regulations. These laws establish a broad regulatory framework governing the privacy and security of PHI. The HIPAA Security Rule establishes 22 separate technology-neutral security standards, which include administrative, physical, and technical safeguards for electronic PHI (ePHI). Each of the standards comprises numerous implementation specifications that must be addressed in protecting the covered entity's ePHI from reasonably anticipated threats and hazards.[8]

Health insurers are required to protect the security of their financial information, defined as "nonpublic personal information," under the Gramm-Leach-Bliley Act (GLB Act).[9] Health care organizations that maintain credit card data may be required via contracts with major credit card companies or state laws to protect such data according to the best practices established under the Payment Card Industry Data Security Standard (PCI DSS).[10] Certain health care organizations also are subject to Federal Trade Commission (FTC) jurisdiction with regard to the security and privacy of personal information, and may be subject to FTC enforcement of prohibitions against unfair business practices.[11]

In addition to federal standards, health information is generally subject to state privacy and/or security laws. The state statutory and regulatory schemes are extremely diverse. All states have privacy laws, some of which govern information on state residents and others that apply to any information held by companies that do business in the state. A small number of states, including California and Minnesota, have comprehensive health information privacy laws. The rest have sector-specific laws that govern access to medical records and the confidentiality of certain sensitive health information (such as mental health data, genetic data, communicable disease data, or HIV test results.[12] A few states, such as Massachusetts and Nevada, also have data protection laws that mandate security controls for personal information, although many have laws or regulations that govern record retention and the disposal of personal data.[13] A few states have established security requirements for electronic health records (EHR).[14]

Similar to HIPAA, these laws establish fines and civil monetary penalties for violations. Some further provide for a private right of action by citizens for unauthorized access, use, or disclosure of health or medical information. In California, a number of class action lawsuits have been filed in the past two years, alleging violations of the Confidentiality of Medical Information Act (the state privacy law) and seeking damages of $1,000 per person per violation.[15]

The majority of states also have data breach notification laws for health information or other personal information. At the end of 2010, 46 states had enacted legislation governing disclosure of security breaches of personal information, and state agencies and some attorney generals have begun actively enforcing these laws.[16] In many cases, state laws impose sweeping requirements for reporting any unauthorized access, use, or disclosure of medical information or personal information. The reporting and notification deadlines may be much tighter than those imposed under the HITECH Act, which allow for up to 60 days for notification of individuals and the U.S. Secretary of Health and Human Services. Moreover, state laws generally impose civil penalties for breaches of personal or health information, which are in addition to those imposed under the HITECH Act. Given the extensive regulations governing health and other sensitive data commonly maintained by health care organizations, the need for data security is obvious.

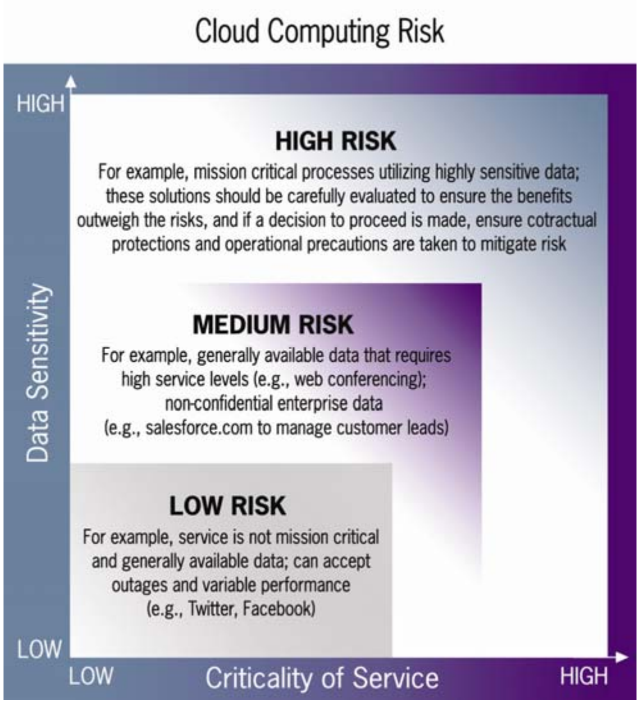
Loss or unauthorized disclosure of such data is a significant concern, because of the liability associated with violations of privacy and security laws. Data breaches have proven to be costly events. A 2010 study examined the costs incurred by 45 organizations after experiencing a data breach, and found an average total cost for a data breach of $6.75 million. Costs averaged from $750,000 for the least expensive data breach event to almost $31 million for the most expensive data breach event, with an average cost of $204 per compromised record.[17] In 2011, a breach at EMC Corporation exceeded that cap and resulted in costs of $66 million, when an intruder stole digital information related to RSA's SecurID authentication products.[18]

In making a business case for protecting PHI, the American National Standards Institute recently developed a formula to project the financial impact to an organization due to breaches of PHI, taking into account the reputational repercussions, the financial repercussions (cost of remediation, communications, insurance coverage, and so forth), and legal/regulatory repercussions to the health care organization. In its hypothetical example, the estimated total cost of an unintentional breach of PHI involving 845,000 medical records was about $26.5 million.[19]

Most important, the overall accountability for the security and privacy of health information cannot simply be delegated to a cloud provider; it remains the obligation of the health care organization. Even though the HITECH Act holds certain subcontractors (referred to as business associates) of covered organizations directly liable for any civil penalties resulting from breaches, state laws and the FTC generally continue to hold organizations responsible for the actions of their subcontractors. Apart from the breach itself, a covered entity may be held liable for a violation of the HIPAA Security Rule if it fails to conduct an adequate risk assessment and implement an adequate risk management process. Therefore the significance of strong contractual protections for data security cannot be overemphasized.

How Should an Organization Evaluate the Risk of Cloud Computing?

Cloud computing involves increased risk associated with certain security vulnerabilities, such as hacking from Web-based interfaces to the network, electronic access to information stored on common servers by different organizations (multi-tenancy), and increased physical risk associated with storage at multiple locations. It also may involve risk of non-performance for service vendors or subcontractors. In addition, there may be increased liability associated with inconsistent rules for data privacy and data breaches across national and state borders and difficulties in attributing liability when a cloud provider subcontracts its services to other vendors. We recommend that risk associated with the decision to implement a cloud computing solution should be evaluated primarily by assessing two variables: (i) the criticality of the business process being supported by the cloud computing solution, and (ii) the sensitivity of the data that will be stored in the cloud. The graph on the following page illustrates this approach.


Cloud Computing Risk
HIGH
Data Sensitivity
LOW
HIGH RISK
For example, mission critical processes utilizing highly sensitive data; these solutions should be carefully evaluated to ensure the benefits outweigh the risks, and if a decision to proceed is made, ensure cotractual protections and operational precautions are taken to mitigate risk
MEDIUM RISK
For example, generally available data that requires high service levels (e.g., web conferencing); non-confidential enterprise data (e.g., salesforce.com to manage customer leads)
LOW RISK
For example, service is not mission critical and generally available data; can accept outages and variable performance (e.g., Twitter, Facebook)
LOW
Criticality of Service
HIGH

When presented with a potential cloud computing solution, simply plot the corresponding points for data sensitivity and criticality of business process on the graph above to quickly get a read on the overall risk profile for the solution. The risk-level assessment should be equated with the highest risk plotted for either variable.

In addition to highlighting the risks associated with cloud computing usage, the objective of this white paper is to provide a framework for evaluating and developing strategies to mitigate those risks.

Specific Recommendations for Managing Cloud Computing Risk

Cloud computing involves accessing a provider's software and infrastructure remotely and often includes storing the customer's data with that provider. To that end, cloud computing agreements have some similarity to traditional software licensing agreements, but often have more in common with hosting or application service provider agreements. As such, the most critical issues and concerns identified with respect to hosting and application service provider agreements are equally applicable to cloud computing agreements.

In a traditional software licensing or hardware purchase engagement, the vendor installs the software or equipment in the customer's environment. The customer has the ability to have the software or hardware configured to meet its particular business needs and retains control over its data. In a cloud computing environment, the software, hardware, and the customer's data are hosted by the provider; the software and hardware configuration is much more homogeneous across all customers; and the data are typically maintained in a shared environment (i.e., many customers per server) unless the customer uses a private cloud solution. Accordingly, the customer's top priorities shift from configuration, implementation, and acceptance to service availability, performance (i.e., service levels), and data security. Like a traditional software licensing or hardware purchase agreement, insurance, indemnity, limitations of liabilities, and warranties remain high priorities as well.

1. PRE-AGREEMENT PROVIDER DUE DILIGENCE

AT A GLANCE

» Pre-agreement due diligence on the provider can provide the customer valuable insight as to whether the provider can meet the customer's expectations.

» In its pre-contract due diligence review, the customer should pay particular attention to the provider's financial condition and track record of corporate responsibility, the provider's use of subcontractors, the location of the data center(s), including disaster recovery, and the provider's security infrastructure and policies and procedures.

The customer should consider performing pre-agreement due diligence on the provider. By crafting and using a provider questionnaire, the customer at the outset can begin to ascertain the extent to which the provider can meet the customer's expectations and, where gaps exist, eliminate or negotiate through them. Examples of the items to address in such a due diligence questionnaire include the provider's financial condition and corporate responsibility, insurance, existing service levels, data security, vendor relationships, location of data, capacity, disaster recovery and business continuity, redundancy, and ability to comply with applicable regulations.

In its pre-contract due diligence review, the customer should pay particular attention to the following issues, which represent a particular risk in a cloud computing environment:

- **The provider's financial condition and corporate responsibility.** Any decisions on whether to entrust a particular cloud provider with the organizations' sensitive data should not be made without considering the provider's financial stability and history of compliance.

- **The provider's use of subcontractors.** Vendor relationships, including the scope of control over the third party, the responsibilities involved (e.g., policy and licensing arrangements), and the remedies and recourse available should problems occur, should be scrutinized if a cloud provider outsources some of its services to third-party subcontractors.

- **The location of the data center(s), including disaster-recovery facilities.** Where the data will be physically stored is important because the location of the data will determine the jurisdiction and the laws governing the data. Offshore data storage involves considerable risk both with respect to the differing privacy and security law, as well as the practical difficulties associated with on-site audits or enforcement of contractual requirements. The location of the data center is just one aspect of the offshore issue. If help desk personnel, programmers, and other provider personnel are located offshore, they also may have access to all data stored in the data center. That is, even if the data center is located in the United States, personnel located offshore may have unrestricted access to that data, increasing the potential risk of misuse.

- **The provider's security infrastructure and policies and procedures.** It is becoming far more common to require providers to demonstrate that their security controls are intact and robust. In any review of the provider's security policies, it is essential that someone competent in data security — either someone within the customer's organization, a data security attorney, or a third-party consultant — be actively involved in reviewing the provider's security policies. Unless the customer clearly knows what controls are necessary to maintain the security of the information and whether the provider's controls satisfy this standard, there is a potential for misguided decision-making. The customer also should consider verifying the provider's capabilities via a physical visit or a third-party audit, or both.

2. SERVICE AVAILABILITY

AT A GLANCE

- In the event that a provider stops delivering services to a customer, the customer will have no access to the services (which may be supporting a critical business function) and, perhaps more important, no access to the customer's data stored on the provider's systems.

- For certain health care providers, such as hospitals, it is critical to be able to continue to operate their business and have access to medical information at all times.

- Customers should ensure that they have proper contractual protections to address the various risks relating to service availability. To mitigate risk in this area, the customer should ensure it obtains: (i) disaster recovery and business continuity assurances, (ii) provider's agreement not to withhold services, and (iii) protections against provider financial instability.

In the event that a provider stops delivering services to a customer, whether due to (i) a server being down, (ii) the failure of a telecommunications link, (iii) a natural disaster causing damage to the provider's data center, (iv) the provider withholding services because of a fee dispute, or (v) the provider closing its business because of financial difficulties, the customer will have no access to the services (which may be supporting a critical business function) and, perhaps more important, no access to the customer's data stored on the provider's systems.

For certain health care providers, such as hospitals, it is critical to be able to continue to operate their business and have access to medical information at all times, particularly in times of natural disaster, pandemics, and other similar occurrences. As such, health care providers should ensure that they have proper contractual protections to address the various risks relating to service availability.

A. DISASTER RECOVERY AND BUSINESS CONTINUITY

Disaster recovery and business continuity provisions requiring the provider to demonstrate and promise that it can continue to make the services available even in the event of a disaster, power outage, or similarly significant event should be included in the service agreement. If the provider is maintaining PHI, a disaster recovery plan and an emergency-mode operation plan are required for compliance with the HIPAA Security Rule. In the event of a prolonged outage, continuity of services should be provided through a secondary server, data center, or provider, as appropriate.

By way of illustration, the following is a sample disaster recovery and business continuity provision:

> *Provider shall maintain and implement disaster recovery and emergency mode operation procedures to ensure that the Services are not interrupted during any disaster. Provider shall provide Customer with a copy of its current disaster recovery plan and emergency mode operations plan and all updates thereto during the Term. All requirements of this Agreement, including those relating to security policies, workforce screening and termination, training, and due diligence shall apply to the Provider's disaster recovery site.**

B. WITHHOLDING OF SERVICES

A general provision prohibiting the provider's withholding of services should be included in any cloud computing agreement. The provider should not withhold services related to mission-critical data because of a fee dispute.

An example of a provision prohibiting the withholding of services is provided below:

> *Provider warrants that during the Term of this Agreement it will not withhold Services provided hereunder, for any reason, including but not limited to a dispute between the parties arising under this Agreement.**

C. BANKRUPTCY AND FINANCIAL WHEREWITHAL

Typically, an agreement may include a provision providing the customer the right to terminate the Agreement in the event of a provider bankruptcy, and also may include a separate provision requiring the provider to assist in transition of the services to a third-party provider or to the customer, in the event of expiration or termination of the agreement. However, once the provider has declared bankruptcy, the provider's ability to assist the customer will be limited.

Therefore, if a customer is not confident of a provider's financial stability, the customer should add a provision that enables the customer to identify potential financial issues in advance. For example, a provision requiring the provider to deliver periodic reports on its financial condition would enable the customer to assess ahead of time whether the provider will be able to continue to provide services. If the customer identifies any issues, the customer has an opportunity to take the appropriate action to minimize any negative impact.

Provided below is a sample "financial wherewithal" provision:

> *Quarterly, during the Term, Provider shall provide Customer with all information reasonably requested by Customer to assess the overall financial strength and viability of Provider and Provider's ability to fully perform its obligations under this Agreement. In the*

> *event Customer concludes that Provider does not have the financial wherewithal to fully perform as required hereunder, Customer may terminate this Agreement without further obligation or liability by providing written notice to Provider.**

3. SERVICE LEVELS

AT A GLANCE

- One of the most critical aspects in contracting for cloud computing services is establishing appropriate service levels in relation to the availability and responsiveness of the services.
- In addition to obtaining an appropriate uptime service level, it is critical that the customer establish an acceptable service level for performance and responsiveness of the services, as services that fail to provide timely responses to its users are effectively unavailable.
- The most common service level issues that the customer should address are: (i) uptime, (ii) service response time, (iii) simultaneous visitors, (iv) problem response time and resolution time, (v) data return, and (vi) remedies.

One of the most critical aspects in contracting for cloud computing services is establishing appropriate service levels in relation to the availability and responsiveness of the services. Because the software and infrastructure are hosted by the provider, outside the control of the customer, service levels serve two main purposes. First, service levels assure the customer that it can rely on the services in its business and provide appropriate remedies if the provider fails to meet the agreed service levels. Second, service levels provide agreed-upon benchmarks that facilitate the provider's continuous quality improvement process and provide incentives that encourage the provider to be diligent in addressing issues. The most common service level issues that the customer should address are: (i) uptime, (ii) service response time, (iii) simultaneous visitors, (iv) problem response time and resolution time, (v) data return, and (vi) remedies.

A. UPTIME SERVICE LEVEL

The provider needs to provide a stable environment where the services are available to the customer at all times as needed to support the customer's business. The uptime service level addresses this issue by having the provider agree that the services will have an uptime (i.e., availability) of a certain percentage, during certain hours, measured over an agreed-upon period.

The specific service level targets depend on the facts and circumstances in each case. However, if health care information is in the cloud, customers should negotiate terms that address their particular business needs.

A customer should carefully consider the outage measurement window (e.g., daily, monthly, quarterly). Providers tend to want longer measurement periods because they dilute the effects of a downtime and thus make remedies less available to the customer. Health care entities using cloud providers for key services, including hosting health data, should have more frequent measurements.

If the cloud provider is hosting a hospital EHR system, service availability is needed 24-hours a day, seven days a week. The agreement should clearly and specifically address this level of service availability. Customers may request the provider be proactive in detecting downtime by explicitly requiring the provider to constantly monitor the "heartbeat" of all its servers through automated pinging. Requiring the provider to do this should result in the provider knowing very quickly that a server is down without having to wait for a notice from the customer. Finally, the concept of "unavailability" also should include severe performance degradation and inoperability of any service feature — see the next section on Service Response Time.

By way of illustration, here is an example of an uptime service level provision:

> *Provider will make the Services Available continuously, as measured over the course of each calendar month, an average of 99.99 percent of the*

> *time, excluding unavailability as a result of Exceptions, as defined below (the "Availability Percentage"). "Available" means the Services shall be available for access and use by Customer. For purposes of calculating the Availability Percentage, the following are "Exceptions" to the service level requirement, and the Services shall not be considered Un-Available, if any inaccessibility is due to: (i) Customer's acts or omissions; or (ii) Customer's Internet connectivity.**

B. SERVICE RESPONSE TIME

Closely related to and, in fact, often intertwined with the uptime service level is the response time service level. This service level sets forth maximum latencies and response times for a customer's use of the services. Providers that fail to respond in a timely manner to its users are effectively unavailable. As with the uptime service level, the specific service level response target depends on the facts and circumstances in each case, including the complexity of the transaction at issue, the processing required, and how critical speed is to achieving the customer's business objectives.

For example, if a customer is accessing services over an Internet connection, then it is recommended that the service level be set in terms of the Keynote Business 40 Internet Performance Index, which measures the average download time for 40 important business Web sites. However, if the services are accessed over a leased line, then the Keynote Business 40 Internet Performance Index may be supplemented or replaced by imposing a response time requirement measured at the provider's external router.

An example provision for a response time service level is provided below:

> *The average download time for each page of the Services, including all content contained therein, shall be within the lesser of (i) 0.5 seconds of the weekly Keynote Business 40 Internet Performance Index ("KB40") or (ii) two (2) seconds. In the event the KB40 is discontinued, a successor index (such as average download times for all other customers of Provider) may be mutually agreed upon by the parties.**

If the provider does not commit to some form of service response time service level, then the customer should ask that the provider at least share its history of response time measurements and should establish some ongoing management of risk in this area. For example, the parties may agree to conduct an end-user satisfaction survey, and agree to take action to improve any user dissatisfaction with respect to service response.

C. SIMULTANEOUS VISITORS SERVICE LEVEL

If the customer expects the services to support multiple simultaneous users, then a service level should be included to explicitly specify such requirement.

D. PROBLEM RESPONSE TIME AND RESOLUTION TIME SERVICE LEVELS

The provider's obligation to resolve issues in a timely manner should be included in any cloud computing agreement. Providers often include only a response time measurement, meaning the time period from when the problem is reported to when the provider notifies the customer and begins working to address the issue. These obligations typically fall short of what is necessary. The agreement also should include a resolution time measurement, meaning the period from when the problem is reported to when the provider implements a fix or acceptable workaround.

E. DATA RETURN SERVICE LEVEL

For services involving a critical business function or sensitive customer information, such as health information, the customer also should consider adding a service level that measures the time between the customer's request for data and the provider's return of such data. This will incentivize the provider to provide the customer data in accordance with the timeframe requirements of the agreement, and provide additional assurance to the customer that it will be able to operate in the event that the provider stops providing services.

F. REMEDIES

Typically, remedies for failure to hit a service level start out as credits toward the next period's service. For example, a remedy might provide: For every X increment of downtime below the agreed-upon level in the measurement period, or for every Severity Level 1 support issue provider does not resolve within the stipulated time, customer receives a credit of five percent of the next month's bill, up to a maximum credit of 75 percent. Depending on the services furnished by the cloud provider, the customer should have the right to implement increasing financial penalties or to terminate the agreement without penalty if the provider does not satisfy the service level, and not have to wait for the current term to expire.

Here is a portion of a sample remedy provision for a service level failure:

> *In the event the Services are not Available 99.99 percent of the time but are Available at least 99 percent of the time, then in addition to any other remedies available under this Agreement or applicable law, Customer shall be entitled to a credit in the amount of $_____ each month this service level is not satisfied. In the event the Services are not Available at least 99 percent of the time, then in addition to any other remedies available under this Agreement or applicable law, Customer shall be entitled to a credit in the amount of $_____and shall be entitled to terminate this Agreement upon written notice to Provider with no further liability, expense, or obligation to Provider.**

4. DATA SECURITY

AT A GLANCE

- The security of a customer's data in a cloud computing environment has been recognized as one of the largest areas of concern for a customer, as the customer is ultimately accountable for complying with privacy and security regulations, and data security breaches have proven to be costly events for organizations.
- HIPAA Business Associate Agreements (BAAs) do not adequately address the data security risks associated with a cloud computing environment and may require additional terms. Contracts between health care organizations and cloud providers should expressly address the provider's infrastructure, including: (i) security policies and procedures, (ii) subcontracting arrangements, (iii) location of data, (iv) breach notification, (v) data redundancy (including data back-up procedures), (vi) data ownership and use of customer data, (vii) e-discovery, (viii) data conversion and return of customer data, and (ix) audit rights (including a requirement that the provider furnish copies of its external auditor's reports).

A. BUSINESS ASSOCIATE AGREEMENTS

Under HIPAA and the HITECH Act, EHR vendors, computer software companies, Health Information Exchanges, and many other providers that are responsible for data analysis, processing, or storage, are considered Business Associates.[20] According to the federal Office for Civil Rights (OCR), a software company that hosts the software containing PHI on its own server, or accesses PHI when troubleshooting the software function, is considered a Business Associate of a covered entity.[21]

Prior to allowing another organization to access its PHI, covered entities must enter into a service agreement or a separate Business Associate Agreement (BAA), which incorporates particular provisions as established by the HIPAA Privacy Rule related to the permitted uses and disclosures of PHI and the security safeguards that must be implemented. If a large health care organization is contracting with an EHR vendor and outsourcing its data storage, the customer may have the ability to negotiate specific protections for its

Customer Information in its BAA. However, smaller organizations such as medical groups that contract with EHR vendors may be presented with an end-user license agreement (EULA) that incorporates the minimum BAA provisions required under HIPAA. Consultation with legal counsel is an important step prior to entrusting an EHR vendor with high-risk, mission-critical data, based on the BAA terms incorporated in an EULA. Even in a standard BAA, the provisions required by HIPAA do not fully address the data security risks associated with a cloud computing environment. The key data security provisions that should be addressed in either the BAA or the service agreement are described below.

The provisions of the BAA should take precedence over the generic confidentiality and security provisions of the cloud provider's form contract.

B. DATA SECURITY

The cloud provider's use of customer data and the security and confidentiality of that customer data are very important in cloud computing agreements. Contracts between health care organizations and cloud providers should expressly address the provider's infrastructure, including: (i) security policies and procedures; (ii) subcontracting arrangements, (iii) location of data, (iv) breach notification, (v) data redundancy (including data back-up procedures), (vi) data ownership and use of customer data, (vii) e-discovery, (viii) data conversion and return of customer data, and (ix) audit rights (including a requirement that the provider furnish copies of its external auditor's reports).

Customers should demand that agreements include specific contractual details about data security, specifically hardware, software, and security policies. To determine whether a provider's security controls are adequate, the customer should compare the provider's policies to its own or map the security controls to the legal requirements. With respect to health data, the safeguards included in a HIPAA-compliant BAA may not satisfy state privacy law requirements. Even if the provisions meet the organizations' legal compliance requirements, the standards established by law are generally baseline security measures. A customer's policies could be more stringent or more specific (or both), and many customers demand that the provider match the customer's policies.

In addition to establishing the standard security procedures, the provider's policies should address security risks particular to cloud computing and services being delivered over the Internet and accessible through a Web browser (e.g., security risks relating to Adobe® Flash®, which allows hackers to upload malicious Flash objects and launch attacks on users). Workforce screening and training policies also should be subject to increased scrutiny when data storage is being outsourced to a cloud provider, in particular if the data are being stored in multiple locations with physical access by multiple parties. Security compliance in a cloud computing environment also involves clearly documenting who is responsible for particular security management tasks. The scope of the customer's and provider's security responsibilities will vary, depending on the services furnished by the cloud provider. For example, if the customer contracts with the cloud provider for Infrastructure-as-a-Service, the cloud provider may be responsible for the majority of security controls to protect the data. On the other hand, if the customer's contract with the cloud provider is limited to Software-as-a-Service, the customer may retain certain responsibilities for security controls (e.g., setting passwords, granting access rights, and so forth). In any relationship with a cloud provider, it is crucial that the scope and nature of the individual and mutual security responsibilities of the respective organizations be understood and documented in the agreement.

To ensure that policy and procedures are being enforced, the cloud provider agreement should include some means for the customer to monitor the security controls and processes employed by the cloud provider and its performance over time. For example, the agreement could include the right to audit, via a third party, security control aspects that are not otherwise accessible or assessable by the consumer. The customer also may request alerts, notifications, and/or reports on the security of the system.

Consider the following sample data security provision:

> *(i) In General. Provider will maintain and enforce administrative safeguards pursuant to 45 C.F.R. § 164.306, technical safeguards pursuant to 45 C.F.R. § 164.308, physical safeguards pursuant to 45 C.F.R. § 164.310, and policies and procedures pursuant to 45 C.F.R. § 164.316 that reasonably protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity, as required by the Security Rule. Further, Provider (a) will maintain and enforce security procedures that are (1) at least equal to industry standards for such types of data and locations, (2) in accordance with reasonable Customer security requirements, and (3) which provide reasonably appropriate physical, technical, and administrative safeguards against accidental or unlawful destruction, loss, alteration, or unauthorized access, acquisition, use, or disclosure of Customer Information and all other data owned by Customer and accessible by Provider under this Agreement. Provider shall comply with all requirements of the HITECH Act related to privacy and security that apply to covered entities, as that term is defined in HIPAA.*
>
> *(ii) Storage of Customer Information and Security Controls. All Customer Information must be stored in a physically and logically secure environment that protects it from unauthorized access, modification, theft, misuse, and destruction. In addition to the general standards set forth above, Provider will maintain an adequate level of physical security controls over its facility. Further, Provider will maintain an adequate level of administrative, technical, and physical data security controls. See Exhibit A for detailed information on Provider's security policies protections.*
>
> *(iii) Security Audits. During the Term, Customer or its third-party designee may, but is not obligated to, perform audits of the Provider environment, including unannounced penetration and security tests, as it relates to the receipt, maintenance, use, or retention of Customer Information. Any of Customer's regulators shall have the same right upon request. Provider agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.**

C. SUBCONTRACTING ARRANGEMENTS

Third-party relationships should be disclosed in advance of reaching an agreement with the cloud provider, and the terms of any relationships that are disclosed and approved by the customer should be maintained throughout the agreement or until sufficient notification can be given of any anticipated changes.

If the provider is not operating the data center itself (e.g., the provider is the owner of the software and will be providing support, but is using a third-party data center to host the software), then the provider should be required to (i) ensure that the third-party host complies with the terms of the agreement (including the data security requirements), (ii) accept responsibility for all acts of the third-party host, and (iii) be jointly and severally liable with the third-party host for any breach by the third-party host of the agreement. Also, the customer should consider entering into a separate confidentiality and non-disclosure agreement with the third-party host for the protection of the customer's data. This can take the form of a simple non-disclosure agreement and, if applicable, BAA. If the provider ever desires to change the host, the provider should be required to provide the customer with advance notice, and the customer should be given time to conduct due diligence with regard to the security of the proposed host and the right to reject any proposed host.

Finally, to comply with HIPAA, the agreement must ensure that any subcontractors to whom the covered entity provides PHI agree in writing to the same restrictions and conditions that apply to the Business Associate in its agreement with the customer.

D. LOCATION OF DATA

The location of the data may determine the jurisdiction and the law governing the data. For example, if personally identifiable information is located in Europe, then European law may govern that information regardless of what is provided for in the contract. Even if the data center is located in the United States, help desk personnel accessing the data could be located in a foreign country with limited or different security and privacy laws. In addition to the difference in laws, location of data overseas also may present practical difficulties with respect to the conduct of on-site audits, enforcement of contractual provisions, and, even accessing customer data (and, on termination of the agreement, ensuring the customer data has been properly deleted from the provider's systems).

Further, Medicare Advantage (MA) plans and Medicare Prescription Drug Plan (PDP) sponsors must satisfy specific Centers for Medicare and Medicaid Services (CMS) requirements with respect to offshore work. If plans or sponsors use offshore subcontractors or permit participating providers to do so, they must submit to CMS specific and detailed attestations for each offshore subcontractor they have engaged to perform Medicare-related work regarding how they have addressed the risks associated with the use of subcontractors operating outside the United States. To ensure compliance, some MA plans or PDP sponsors include broad prohibitions against offshore work (which may include prohibitions on access to data by workers outside the United States) in their network participation agreements.[22]

Even if the data center is in the United States, the customer should consider where the data center is located. When information crosses state borders, the governing legal, privacy, and regulatory regimes can differ significantly and raise a variety of concerns. The main concern is which state laws apply to the data and whether those laws represent any additional compliance requirements, liabilities, or benefits. For example, Nevada's data protection law applies to organizations doing business in the state, including having operations, customers, or employees in Nevada.[23] California medical privacy laws apply to, among others, businesses organized for the purpose of maintaining medical information; these businesses are subject to the same penalties as health care providers for improper use and disclosure of medical information.[24]

At minimum, the customer should consider adding a restriction against offshore work and data flow to foreign countries, including a requirement that the data center (including the hosted software, infrastructure, and data) be located and the services be performed in the United States, and that no data be made available to those located outside the United States. Although providers will seek to maintain the flexibility to move data among their various facilities, including those of their contractors, depending on their needs, customers should carefully consider such provision and restrict cloud computing providers from transferring data from the specific agreed-upon location without advance notice of the customer.

Below is a sample provision prohibiting offshore work and transfer of data.

> *In performing the functions, activities or services for, or on behalf of, Customer, Provider shall not, and shall not permit any of its subcontractors, to transmit or make available any PHI to any entity or individual outside the continental United States without the prior written consent of Customer. All activities and services shall be performed and rendered at the locations set forth in Attachment __. The Parties may mutually agree to authorize Provider's use of additional locations in an amendment to this Agreement.**

E. BREACH NOTIFICATION

State and federal laws may include multiple, distinct reporting requirements (e.g., HIPAA requires reporting of security incidents, impermissible uses and disclosures of PHI, and breaches). Therefore, a key issue in a cloud computing agreement is investigation and notification of any breach of the security of customer information, so that the customer can appropriately notify individuals and regulatory agencies. Beyond establishing the procedural requirements and timeframes for reporting to the customer, the agreement should set forth the procedures and role of the parties with respect to investigation of the breach and notification of individuals. The customer should retain sole control of the timing, content, and method of notification. More significantly, the agreement should address the liability for breaches. If the provider is responsible for the breach, then the agreement should require the provider to reimburse customer for its reasonable out-of-pocket costs in providing the notification and mitigating the harm and indemnify the customer for any damages, costs, fines, and penalties related to the breach.

Below is a sample provision for notification of security incidents, impermissible uses and disclosures of PHI, and breaches under HIPAA. The BAA or service agreement should include similar provisions to address notification of impermissible uses of customer information or breaches under other state or federal laws.

> *i. Provider shall investigate each unauthorized access, acquisition, Use, or Disclosure of Customer's PHI that it discovers to determine whether such unauthorized access, acquisition, Use, or Disclosure constitutes a reportable Breach of Unsecured PHI. If Provider determines that a reportable Breach of Unsecured PHI has occurred, Provider shall notify Customer of such Breach in writing without unreasonable delay but no later than thirty (30) calendar days after discovery of the Breach, in accordance with 45 C.F.R. § 164.410(c). Provider shall cooperate with Customer in meeting Customer's obligations under the HITECH Act with respect to such Breach. Customer shall have sole control over the timing and method of providing notification of such Breach to the affected individual(s), the Secretary and, if applicable, the media, as required by the HITECH Act. Provider shall reimburse Customer for its reasonable costs and expenses in providing the notification, including, but not limited to, any administrative costs associated with providing notice, printing and mailing costs, and costs of mitigating the harm (which may include the costs of obtaining credit monitoring services and identity theft insurance) for affected individuals whose PHI has or may have been compromised as a result of the Breach.*

> *ii. Provider shall report to Customer's Privacy Officer each Use or Disclosure that is made by Provider, its Workforce, or agents or subcontractors that is not specifically permitted by this Agreement within five (5) days of the time that it becomes aware. In addition, Provider shall report to Customer's Privacy Officer each Security Incident, as defined in HIPAA, of which it becomes aware within seventy-two (72) hours from such time.**

F. DATA REDUNDANCY

Because the customer relies on the provider as the custodian of its data, the customer should demand the cloud computing agreement contain explicit provisions regarding (i) the provider's duty to back up customer data and the frequency of that back up, and (ii) the customer's ongoing access to such data or the delivery of such data to the customer on a regular basis. A good place to start is for the customer to compare the provider's back-up policies to its own and make sure they are at least as stringent. If the data constitutes PHI or is otherwise business-critical, then the cloud provider must have in place a written data back-up plan.

Below is a sample data redundancy provision:

> *Provider will: (i) execute (a) nightly database back-ups to a back-up server, (b) incremental database transaction log file back-ups every 30 minutes to a back-up server, (c) weekly back-ups of all hosted Customer Information and the default path to a back-up server, and (d) nightly incremental back-ups of the default path to a back-up server; (ii) replicate Customer's database and default path to an off-site location (i.e., other than the primary data center); and (iii) save the last 14 nightly database back-ups on a secure transfer server (i.e., at any given time, the last 14 nightly database back-ups will be on the secure transfer server) from which Customer may retrieve the database back-ups at any time.**

G. DATA OWNERSHIP AND USE RIGHTS

Detailed provisions should be added to clarify that customer owns all data stored by the provider for the customer. In the event that the provider stops providing services, there should be no separate dispute as to ownership of the data that resides on the provider's servers. If the cloud provider has access to the customer's personal information or health information, the agreement must contain specific language (i) regarding the provider's obligations to maintain the confidentiality of such information and (ii) placing appropriate limitations on the provider's use of such customer information (i.e., confirming that the provider has no right to use such information except in connection with its performance under the cloud computing agreement).

Many cloud computing providers want to analyze and use the customer data that resides on their servers for their own commercial benefit, and, in particular, the data customers create as they use the services. For example, the provider may wish to use a customer's data, aggregated along with other customers' data, to provide data analysis to industry groups or marketers. However, there may be legal restrictions on the creation or use of aggregated data.

Customers may conclude that the provider should not have any right to use the customer's data, whether in raw form, aggregated, or de-identified, beyond what is strictly necessary to provide the services. An example in which a commercial use might be acceptable is where the provider furnishes a service that depends on the ancillary use of data from other customers, such as aggregating customer data to provide data trending and analysis of health care quality to the customer and similarly situated customers who share a relationship to an individual. This use would be permissible as health care operations under HIPAA. However, the agreement should clearly establish the permissible uses and disclosures of the PHI and should restrict the uses of the aggregated data. Similarly, the agreement may apply certain restrictions to customer data in general.

H. E-DISCOVERY

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic-discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. Some cloud computing providers utilize a practice called de-duplication which removes redundant data from customer files to save storage space in the provider's network. If a customer uploads a file to the provider's network and then later retrieves that file, while it may not appear the content of the file has been altered, the de-duplication process may have removed "meta data" from the file (i.e., data about the file, such as who created it, when it was created or last modified, and so forth.). The removal of this "hidden" information can result in many issues in the event of litigation. For example, if the customer has agreed to produce meta data in response to an electronic discovery (or e-discovery) request and later finds the data is missing or has been altered, the customer may find itself subject to sanctions in the litigation. In addition, meta data (such as dates and comments) may be useful as evidence at trial, and the customer may not be able to rely on such evidence if it is removed or altered by the cloud computing provider. Further, the file itself may not be admissible as evidence, as the removal of the meta data may bring into question the authenticity of the electronic document in its entirety. The cloud provider's electronic discovery capabilities and processes must not compromise the privacy or security of the data and applications of the organization in satisfying the discovery obligations of other cloud consumers, and vice versa. The customer should discuss these issues with the provider, and ensure its cloud computing agreement does not contain terms and conditions allowing removal of meta data from files stored in the provider's network.

I. DATA CONVERSION/RETURN OF DATA

Data conversion, both at the onset and termination of the cloud computing agreement, must be addressed to avoid hidden costs and being "locked in" to the provider's solution. Going into the relationship, the customer should confirm that its data can be directly imported into the provider's services or that any data conversion needed will be done at provider's cost or at customer's cost (with customer's agreement). A customer should consider conducting a test run of provider's mapping scheme to see how easy or complicated it will be (likewise when checking provider's references, a customer should ask about data migration experiences). The customer does not want to be trapped into staying with provider because of data format issues. Nor does it want the provider to retain a copy of its data indefinitely, because the customer's liability associated with the confidentiality of such data would extend beyond the expiration date of the contract for services. To that point, the agreement should include explicit obligations on the part of the provider to return the customer's data, both in the provider's data format and in a platform-agnostic format, and thereafter securely and irretrievably destroy all of the customer's information on the provider's servers upon expiration or termination of the agreement.

A sample data conversion provision is provided below:

> *At Customer's request, Provider will provide a copy of Customer Information to Customer in an ASCII comma-delimited format on a CD-ROM or DVD-ROM Upon expiration of this Agreement or termination of this Agreement for any reason, Provider shall (i) deliver to Customer, at no cost to Customer, a current copy of all of the Customer Information in use as of the date of such expiration or termination and (ii) completely destroy or erase all other copies of the Customer Information in Provider's or its agents' or subcontractors' possession in any form, including but not limited to electronic, hard copy, or other memory device, using methods at least as protective as the DoD 5220-22-M Standard or NIST Special Publication 800-88, Guidelines for Media Sanitization. At Customer's request, Provider shall have its officers certify in writing that it has so destroyed or erased all copies of the Customer Information and that it shall not make any use of the Customer Information.**

5. INSURANCE

AT A GLANCE

- The customer should self-insure against IT risks by obtaining a cyber-liability policy.
- In addition, the provider should be required to carry the following forms of liability insurance: (i) Technology Errors and Omissions Liability Insurance, and (ii) Commercial Blanket Bond, including Electronic & Computer Crime or Unauthorized Computer Access Insurance.

The customer should always address insurance issues in cloud computing situations, both as to the customer's own insurance policies and the provider's insurance. Many data privacy and security laws will hold the customer liable for a security breach, whether it was the customer's fault or the provider's fault. If the law holds the cloud provider liable for the breach and associated civil penalties, the customer may still face liability if the breach results in lawsuits or if there is any allegation that the customer failed in its obligations for security management. Thus, the customer should help self-insure against IT risks, including data and privacy issues, by obtaining a cyber-liability policy.

Cyber-liability insurance can protect the customer against a wide range of losses. Most cyber insurance policies will cover damages arising from unauthorized access to a computer system, theft or destruction of data, hacker attacks, denial of service attacks, and malicious code. Some policies also cover privacy risks like security breaches of personal information, may apply to violations of state and federal privacy regulations, and may provide reimbursement for expenses related to the resulting legal and public relations expenses.

The customer also should require the provider to carry certain types of insurance, as adequate cyber-liability insurance enhances the likelihood that the provider can meet its obligations and provides direct protection for the customer. The primary forms of liability insurance that a provider should be required to carry are: (i) Technology Errors and Omissions Liability

Insurance and (ii) Commercial Blanket Bond, including Electronic & Computer Crime or Unauthorized Computer Access Insurance. These types of insurance will cover damages the customer or others may suffer as a result of the provider's professional negligence and intentional acts by others (e.g., provider's employees, hackers, and so forth.). It is critical that the customer require the provider have these types of policies and not just a general liability policy. Many commercial general liability policies contain a professional services exclusion that precludes coverage for liability arising from IT services as well as other exclusions and limitations that make them largely inapplicable to IT-related risks. The customer also should consider requiring the provider to list customer as an additional insured on its polices; doing so allows the customer to go directly against the provider's insurance company in the event of a claim.

6. INDEMNIFICATION

AT A GLANCE

» The provider should indemnify the customer against damages, lost profits, fines, sanctions, penalties, costs, or expenses resulting from a breach by the provider of its obligations for the confidentiality and security of the customer's data.

The provider should agree to defend, indemnify, and hold harmless the customer and its affiliates from any damages, lost profits, fines, sanctions, penalties, costs, or expenses resulting from a breach by the provider of its obligations in regards to the confidentiality and security of the customer's data. The provider may have to attempt to negotiate a cap on its potential for losses, lost profits, or any other indirect damages. The customer should carefully consider any limitation on liability, and should bargain for no limit on the provider's responsibility. The provider also should agree to defend, indemnify, and hold harmless the customer and its affiliates and agents from any claim that the services infringe the intellectual property rights of any third party. This means that the customer will have no out-of-pocket costs or expenses if some third-party claims infringement. Providers often try to limit the intellectual property indemnification only to infringement of copyrights. That is not acceptable, as many infringement actions arise out of patent or trade secret rights. The indemnity should extend to infringement claims of any "patent, copyright, trade secret, or other proprietary rights of a third party." In addition, customers should avoid any restriction to patents "issued as of the Effective Date" of the agreement. Providers also usually limit the indemnification to "United States" intellectual property rights, and that is generally acceptable, but the customer should consider whether its use of the services will occur overseas.

7. LIMITATION OF LIABILITY

AT A GLANCE

» Limitation of liability clauses must be carefully scrutinized.

» While a customer will not likely be able to eliminate the limitation of liability in its entirety, the customer should seek the following concessions: (i) mutual protection (i.e., application of the limitation of liability to both provider and customer, not just provider), (ii) carve-outs for particularly important areas (e.g., confidentiality, security, indemnity), and (iii) a reasonable liability cap for direct damages.

The provider's limitation of liability is very important in a cloud computing engagement because virtually all aspects of data security are controlled by the provider. Thus, the provider should not be allowed to use a limitation of liability clause to unduly limit its exposure. Instead, a fair limitation of liability clause must balance the provider's concern about unlimited damages with the customer's right to have reasonable recourse in the event of a data breach or other incident.

A provider's limitation of liability clause usually (i) limits any liability of provider to the customer to the amount of fees paid under the agreement or a portion of the agreement (e.g., fees paid for the portion of the services at issue), and (ii) excludes incidental, consequential (e.g., lost revenues), exemplary, punitive, and other indirect damages. While a customer may not be able to eliminate the limitation of liability in its entirety, the customer should ask for concessions.

Provided below are possible concessions the customer should ask for when negotiating the limitation of liability provision:

- The limitation of liability should apply to both parties. The customer should be entitled to the same protections from damages that the provider is seeking
- The following should be excluded from all limitations of liability and damages: (i) breach of the confidentiality and security provision by either party; (ii) the parties' respective third-party indemnity obligations; (iii) either party's infringement of the other party's intellectual property rights; and (iv) breach of the advertising/publicity provision (see item 12 below titled "Publicity")
- The overall liability cap (usually limited to fees paid) should be increased to some multiple of all fees paid (e.g., two to four times the total fees paid or the fees paid in the 12 months prior to the claim arising). Customer should keep in mind that the overall liability cap should not apply to the exclusions in the bullet point above

8. INTELLECTUAL PROPERTY

AT A GLANCE

- Whether the provider will be performing significant implementation services or simply making modifications to configurable screens based on customer's direction, the customer should be aware of its intellectual property rights and the impact of those rights on its business.

The customer needs to understand the impact of intellectual property rights on its business. In the event the provider will be performing significant implementation services in connection with the cloud computing services, the intellectual property ownership structure proposed by a provider may not effectively address the customer's business needs. If the provider's intellectual property is incorporated into work product delivered to the customer, then such provider's intellectual property may be embedded in the customer's business processes as a result. This could encumber the customer's business by creating uncertainty about the customer's rights to such processes on which the business depends. Therefore, the customer should obtain ownership of any "work product" and a very broad license to use any provider intellectual property incorporated into any work product, so that it is able to remain in sole control of the direction of its business and each of its underlying processes.

Even in the case where significant implementation services are not being provided, and the customer is merely providing direction as to configurable screens that will be used by the customer, the customer should realize the potential impact on its business. As a provider may benefit from such ideas provided by the customer, the customer should consider adding a restriction against the provider using those same ideas in services being delivered from provider to any of customer's competitors.

9. WARRANTIES

AT A GLANCE

- The customer should seek to obtain warranties related to conformance to specifications, provider performance, third-party intellectual property infringement, no pending litigation, and so forth.

There are several warranties that are typically included in a cloud computing agreement. The following is a list of warranties that the customer should seek to obtain:

- The services will materially conform to the specifications and, to the extent not inconsistent with the specifications, provider's documentation.
- All services will be provided in a professional, competent, and timely manner by appropriately qualified provider personnel in accordance with the agreement and consistent with provider's best practices.
- The provider will provide adequate training, as needed, to customer on the use of the services.

- The services will comply with all federal, state, and local laws, rules, and regulations.
- The customer's data and information will not be shared with or disclosed in any manner to any third party by provider without first obtaining the express written consent of customer.
- The services will not infringe the intellectual property rights of any third party.
- The services will be free from viruses and other destructive programs.
- There is no pending or threatened litigation involving provider that may impair or interfere with the customer's right to use the services.
- The provider has sufficient authority to enter into the agreement and grant the rights provided in the agreement to the customer. If the provider will be making the customer data available outside the United States and the customer is willing to assume that risk, the provider should warrant that it is fully responsible for complying with all laws and regulations in the relevant jurisdictions relating to transfer of personal data across their borders.

10. LICENSE/ACCESS GRANT AND FEES FOR SOFTWARE

AT A GLANCE

- The grant as to permitted use should be straightforward and broadly worded to allow the customer full use of hosted software and services.
- The agreement should clearly authorize use by all end-users designated by the customer who need to access or use the hosted software and services.

The license or access grant in a cloud computing agreement encompasses three main issues: permitted use, permitted users, and fees. The grant as to permitted use should be straightforward and broadly worded to allow the customer full use of hosted software and services (frequently referred to, collectively, as the "Services"). For example, "Vendor hereby grants Customer a worldwide, non-exclusive license to access and use the Services for Customer's business purposes." Vendor agreements often try to limit the customer's use of the Services to "its internal purposes only." Such a restriction is likely too narrow to encompass all customer's desired uses. Drafting the license in terms to permit the customer to use the Services for "its business purposes" is a better, more encompassing approach.

The license rights related to which customer's constituents can use the Services, and at what price, can be far more complicated. As to permitted users, the customer must carefully define this in light of its needs and its structure. For example, beyond customer's employees, the customer may want affiliates, subsidiaries (now or hereafter existing), corporate parents, and third parties such as outsourcers, consultants, and subcontractors all to have access to the software. The agreement should clearly set forth those users that fit the customer's anticipated needs.

11. IMPLEMENTATION

AT A GLANCE

- When there will be significant implementation services, the client should consider establishing a broad definition of "Services" in the cloud computing agreement.
- This is useful in limiting provider claims of "out of scope" activity and requests for additional money.

In the event significant implementation services are being provided (e.g., extensive software or hardware installation, configuration, or customization services), the definition of "Services" in a cloud computing agreement should be broadly worded to capture all of the contemplated services provided. For example, "'Services' shall mean Provider's provision of software and infrastructure services described in Exhibit __ (Software and Infrastructure Services) and implementation services described in Exhibit __ (Implementation Services), and any other products, deliverables, and services to be provided by Provider to

Customer (i) described in a Statement of Work, (ii) identified in this Agreement, or (iii) otherwise necessary to comply with this Agreement, whether or not specifically set forth in (i) or (ii).” A broad definition of “Services” such as the one above is recommended, as it is useful in limiting provider claims of “out of scope” activity and requests for additional money.

In addition, the customer must fully understand its requirements and the capabilities of the services being provided to determine if any additional features or functionality is needed. Any additional work required to support such features or functionality should be discussed and identified up front, as typically a cloud computing solution may offer more limited configuration and customization options (e.g., multi-tenant application) in order for the provider to more efficiently manage the services and provide a more scalable solution. Any additional work agreed upon to support such features or functionality should be included in the description of services.

12. FEES

AT A GLANCE

» The cloud computing agreement should provide the customer the ability to both add and remove resources, with a corresponding upward and downward adjustment of the service fees.

» In addition, the customer should identify all potential revenue streams and make sure that the identified fees are inclusive of all such revenue streams.

There are many options with respect to pricing, depending on the nature of the services provided, private versus public cloud, required service levels, and so forth. However, typically a cloud computing service will be offered on a pay-as-you-go or pay-per-use cost structure (e.g., per virtual machine each hour, per gigabyte of storage each month, per active user each month). Accordingly, the agreement should provide for the ability to both add and remove resources, with a corresponding upward or downward adjustment to service fees. The best time for the customer to negotiate rates for incremental and decremental use is before signing the agreement. Customers should attempt to lock in any recurring fees for a period of time (one to three years) and thereafter an escalator based on CPI or other third-party index should apply.

In addition, the customer should identify and negotiate all potential additional fees. For example, the provider may attempt to charge additional fees for more storage after a certain amount of data, or additional fees for software updates. The customer should ensure that these are included as part of the negotiated fees.

13. TERM AND TERMINATION

AT A GLANCE

» The customer should be able to terminate the agreement at any time without penalty upon reasonable notice (e.g., 14 to 30 days).

» If the agreement involves PHI, the BAA should permit immediate termination upon knowledge of a material breach.

Because the software and infrastructure are being provided as a service, like any service, the customer should be able to terminate the agreement at any time without penalty upon reasonable notice (e.g., 14 to 30 days). The provider may request a minimum commitment period from the customer to recoup the provider’s “investment” in securing the customer as a customer (i.e., sales expenses and related costs). If the customer agrees to this, then the commitment term should be no more than one year and the provider should provide evidence of its up-front costs to justify such a requirement. However, HIPAA requires that a covered entity be permitted to terminate the agreement upon knowledge of a material breach by a subcontractor, unless the subcontractor is able to cure the breach. Therefore, if the cloud computing services involve use or disclosure of PHI, the BAA or service agreement should provide for an exception to the commitment term that permits termination without penalty under these circumstances.

14. ASSIGNMENT

AT A GLANCE

» The cloud computing agreement should allow the customer to assign its rights under the agreement to its affiliates and successor entities.

The customer should be able to assign its rights under the agreement to its affiliates and other entities which may become a successor or affiliate due to a reorganization, consolidation, divestiture, or the like. Any concerns the provider may have about an assignment can be addressed by the requirement that the assignee will accept all of the customer's obligations under the agreement. The cloud provider should be precluded from assignment of its rights and obligations, or the customer should obtain assurance that any provider assignee will agree to be bound by all of the terms and conditions of the agreement, including, without limitation, service level obligations.

15. EXCLUSIVITY

AT A GLANCE

» In order for customers to obtain the best pricing, providers are asking customers to contractually commit to an exclusive engagement.

» Before considering entering into such an arrangement, the customer should ensure that it has the proper protections in the agreement, including excellent service levels, appropriate exceptions to exclusivity, and the right to transition in anticipation of a termination.

More and more providers are seeking exclusivity in their cloud computing contracts. That is, to obtain the best pricing, providers are asking customers to contractually commit to an exclusive engagement in which the customers may not seek similar services from another provider. The challenge of these exclusive arrangements is that if the exclusive cloud provider does not furnish excellent service levels and other protections, the customer could find itself bound to a bad agreement. It could be stuck with a poorly performing provider that the customer cannot terminate and, to compound the problem, the customer would be prohibited from seeking supplemental services from an alternate provider.

There are three primary areas to consider in entering into an exclusive arrangement:

» **Is the provider offering strong service levels?** To commit to an exclusive agreement, the customer must have confidence the cloud services will be available when needed and achieve all other performance requirements. Those service levels should be very clearly defined and not be qualified by dozens of vague exceptions. There also should be realistic credits to ensure the provider has sufficient incentive to achieve required performance levels and a customer termination right for continuing or substantial service level failures.

» **Are there appropriate exceptions to exclusivity?** There are situations that may arise in which the cloud provider cannot perform as required under the agreement, but would not be in breach. For example, the provider may be subject to a force majeure event (a condition beyond the control of the provider, like war or a natural disaster) or other circumstance that temporarily relieves the provider of its performance obligations (e.g., a period in which the provider is operating under its business continuity and disaster recovery procedures). The problem is that the customer may still need to conduct its business during the pendency of the event. In such cases, the customer should be relieved of its exclusivity obligations to the extent necessary to obtain temporary services from an alternate provider Depending on the type of services at issue, if the event continues for more than a few days, the customer should have the right to terminate and permanently transition to an alternate provider.

» **Does the agreement permit transition in anticipation of a termination?** Every cloud agreement will have a defined duration or term (e.g., an initial term of two years, with certain renewal terms). As that term comes to an end, the customer may want to explore a relationship with an alternate provider. To ensure a smooth transition, the customer will likely need the right to enter into an agreement with the alternate provider well before the existing agreement expires. The exclusivity provision should be drafted to include a right for the customer to enter into an agreement with an alternate provider in anticipation of expiration.

Exclusive engagements can provide the customer with potentially substantial pricing advantages. Nevertheless, any time a customer enters into an exclusive relationship, it is increasing the difficulty of making a change to another provider based on performance or pricing or other changes in circumstance. So the advantages of such agreements should be carefully weighed against the overall risk of such a contract.

16. POST-EXECUTION ONGOING PROVIDER ASSESSMENT

AT A GLANCE

» Establishing a regular program of evaluating the provider's performance would allow the customer to perform ongoing risk assessments during the term of the agreement.

Last, it is recommended that the customer and provider agree to implement a regular program to evaluate the provider's performance. Under such a program, the provider would be required to supply the requisite information to assess provider's services, notify the customer of any changes with regard to the provider, and provide any recommendations to improve the services. This information could then be used by the customer to perform ongoing risk assessments and determine whether to continue the provider relationship. Ongoing visibility into performance regarding data security is particularly important, and the customer may require verification of the provider's capabilities on a regular basis, such as through periodic external audits.

Negotiations

If the customer has substantial leverage when negotiating a cloud computing agreement, then the customer should seek to obtain the protections described above. However, in circumstances where the customer does not have such leverage, providers may be resistant to such protections or any modification to its form contract provisions.

To determine whether to adopt a cloud solution, the customer should carefully evaluate the business risks of the proposed arrangement, including whether the services support a critical business function, involve sensitive customer information, or are customer-facing. If the customer is not able to obtain the level of protection needed in the most significant areas of risk, then the customer should consider walking away from the transaction. If walking away is not an acceptable option, then the customer needs to focus on risk mitigation. For example, if the provider refuses to modify its uptime service level, arguing that it cannot separately administer such a service level for different customers, then the customer should negotiate improved remedies and exit rights for a failure of such service level. In this type of situation, where a customer is unable to obtain the appropriate contractual protections and chooses to proceed, the post-execution ongoing assessment of the provider relationship described above becomes even more important. For a health care customer, data security and service levels are essential to the proper handling of sensitive or highly confidential data, and providers that cannot verify that they meet such security standards should be avoided.

Conclusion

In conclusion, as health care organizations move to the cloud to lower costs and achieve service flexibility, there has been a growing recognition of the substantial risks that come with a cloud computing solution. Unlike traditional software licenses and hardware purchase agreements, but similar to hosting and application service provider agreements, the customer needs to focus less on configuration, implementation, and acceptance, and more on service availability, performance, and the security and control of the customer's data. In particular, customers should ensure that their contract with a cloud service provider:

- » Codifies the specific parameters and minimum levels required for each element of the service, as well as remedies for failure to meet those requirements
- » Details the system infrastructure, data storage and maintenance procedures, and security controls to be maintained by the service provider, along with the organization's rights to audit compliance
- » Affirms the organization's ownership of its data stored on the service provider's system, and specifies its rights to get it back
- » Provides for indemnification against breaches and requires that the provider maintain appropriate cyber-liability insurance

By keeping these key business terms in mind, along with the other risk factors and recommendations identified in this white paper, health care customers can more effectively manage and substantially reduce the risks inherent in cloud computing relationships.

Authors

M. Leeann Habte
Los Angeles, California
213.972.4679
lhabte@foley.com

Matthew A. Karlyn
Boston, Massachusetts
617.502.3231
mkarlyn@foley.com

James R. Kalyvas
Los Angeles, California
213.972.4542
jkalyvas@foley.com

Michael R. Overly
Los Angeles, California
213.972.4533
moverly@foley.com

Editors

Michael L. Blau
Boston, Massachusetts
617.342.4040
mblau@foley.com

Richard K. Rifenbark
Los Angeles, California
213.972.4813
rrifenbark@foley.com

Appendix A — Definitions

Forrester Research

"[A] standardized IT capability (services, software, or infrastructure) delivered via Internet technologies in a pay-per-use, self-service way."[25]

Gartner

"[A] style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies."[26]

IDC

"[A] emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet (i.e., enabling cloud services)."[27]

National Institute of Standards and Technology (NIST)

"[A] model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[28]

U.C. Berkeley Reliable Adaptive Distributed Systems Laboratory (RAD Lab)

"[R]efers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS) … . The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the public, we call it a Public Cloud; the service being sold is Utility Computing … . We use the term Private Cloud to refer to internal datacenters of a business or other organization that are not made available to the public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not normally include Private Clouds."[29]

Wikipedia

"Internet- ('cloud-') based development and use of computer technology ('computing') … a new supplement, consumption and delivery model for IT services based on the Internet, and it typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet."[30]

Appendix B — Cloud Computing Features and Comparison

Cloud Computing Features

Although there may be no single widely accepted definition of cloud computing, based on various definitions, the following features are generally common to a cloud computing approach to delivering IT services.

CLOUD

- IT resources are delivered over the Internet "cloud"
  - Note: For purposes of our analysis, we focus on the "public" cloud (i.e., the Internet, which includes the hardware and software systems in the provider's remote data center), as opposed to a "private cloud" (i.e., hardware and software systems in a customer enterprise)
  - IT resources are managed in the provider's remote data center, rather than on the customer's local computers and servers
  - The provider has responsibility for the IT resources, including design, development, procurement, installation, testing, deployment, provisioning, and management

SERVICE

- IT resources are delivered to the customer via the Internet and consumed by the customer as a "service"
  - IT resources include software, software development platforms, and infrastructure (including virtual servers, memory, processors, storage, and network bandwidth)
  - The customer accesses the services using a Web browser or other interface

SCALABLE ON-DEMAND

- IT resources are scaled up and down at the customer's demand
  - Scalability — Ability to scale up to "unlimited" resources
  - Elasticity — Ability to quickly add and remove resources (within seconds or minutes, as opposed to days or weeks)
- Scalability on-demand is often facilitated through use of the following technologies/approaches, which improve resource utilization and allow for a more scalable approach:
  - Virtualization — Relates to creating a layer of abstraction that converts physical computing resources into a virtual pool of resources, which can be shared by different users (e.g., through server virtualization, a single physical server is partitioned into multiple virtual machines each running a separate operating system, such that the computing resources of the underlying physical server are used as a pool of resources by each of the virtual machines)
  - Multi-tenant software architecture — A single instance of software serves multiple customers at the same time, with each customer sharing hardware resources

UTILITY/SUBSCRIPTION BILLING

- Utility billing
  - Payment is based on the amount of resources used, similar to how one is charged for water, electricity, or gas (e.g., per virtual machine each hour, per gigabyte of storage each month, per active user each month)

- Subscription billing
  - Payment is based on a period of time, similar to how one is charged for a newspaper or magazine subscription (e.g., per month)

Is Cloud Computing Just Another Name for Existing Service Delivery Models?

There has been much discussion as to whether cloud computing is just another name for existing service delivery models, including Application Service Provider (ASP) and Software-as-a-Service (SaaS). The confusion over whether cloud computing is any different than ASP or SaaS naturally arises from the fact that cloud computing, as with ASP and SaaS, involves the remote hosting of software and delivery of software services over the Internet. Although there is this significant overlap among the terms, there are some subtle distinctions. While SaaS is often considered a type of service under cloud computing, ASP either can be considered a type of cloud computing service as well or can be distinguished as something very different, depending on how the term "ASP" is defined.

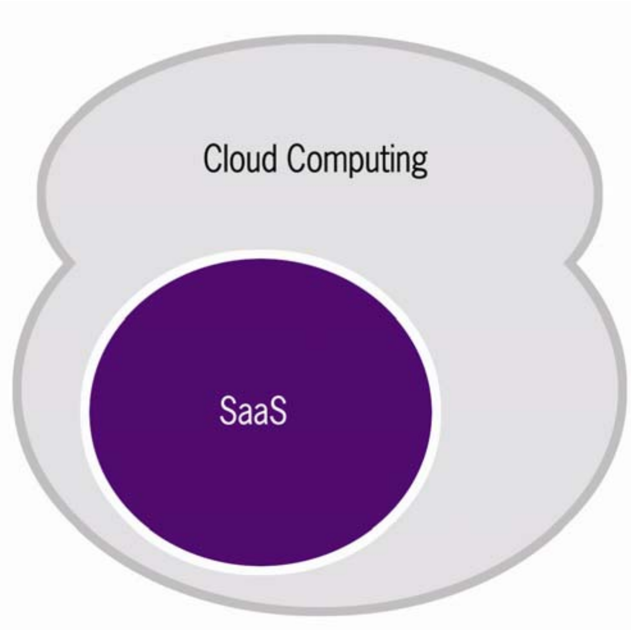
Regardless of whether a solution is ultimately identified as ASP, SaaS, or cloud computing, it is important to note that these solutions share similar critical risk issues and, as a result, a very similar risk analysis applies to each of these service delivery models.

SAAS IS A TYPE OF SERVICE UNDER CLOUD COMPUTING

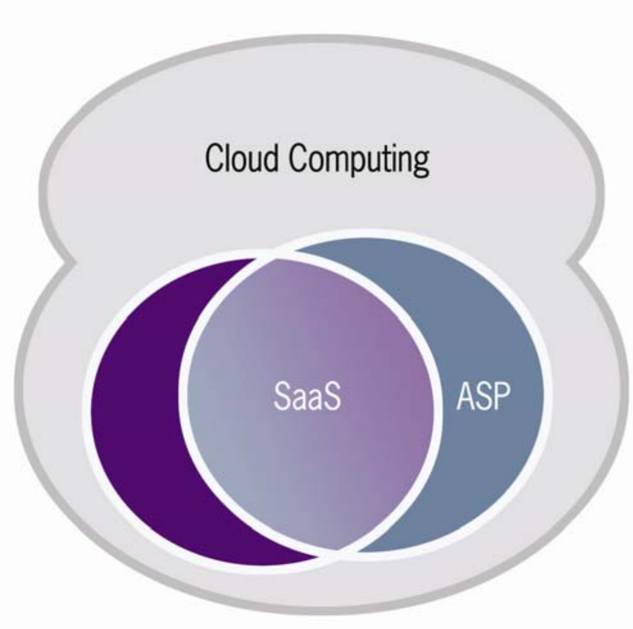
Cloud computing has generally been broken down into three types of services: (i) SaaS, (ii) Platform-as-a-Service (PaaS), and (iii) Infrastructure-as-a-Service (IaaS).

- SaaS — Refers to provider's software being delivered over the cloud to the customer as a service (e.g., Salesforce CRM).
- PaaS — Refers to provider's software development platforms being delivered over the cloud to the customer as a service (e.g., Google App Engine). For example, a customer may use the service to develop, test, and deploy applications that are then hosted on the provider's infrastructure.
- IaaS — Refers to virtual servers, memory, processors, storage, network bandwidth, and other types of infrastructure resources, being delivered over the cloud to the customer as a service (e.g., Amazon Elastic Compute Cloud (EC2)). For example, a customer may use the service to obtain multiple virtual servers to enable a scalable deployment of the customer's own applications.

As a result, SaaS is considered a part of the cloud computing service delivery model.



Many take the position that there is no difference between SaaS and ASP. Therefore, if the term "ASP" is defined as a business model that provides software as a service over the Internet (similar to SaaS), then ASP also would be included as a part of the cloud computing service delivery model.



However, cloud computing may be distinguished from both SaaS and ASP in that it also includes providing software development platforms and infrastructure as a service. Through PaaS, a customer is provided access to a provider's software development platform as a service so that the customer can develop, test, and deploy applications. Through IaaS, a customer is provided the option of purchasing IT infrastructure resources (e.g., servers, storage, and so forth) as a service delivered across the Internet, instead of the customer having to procure such resources for implementation in its local enterprise network.

ASP MAY BE DISTINGUISHED AS A NON-SCALABLE SOLUTION

Some take the position that the ASP and SaaS service delivery models are different. Those taking such a position often define ASP as a business model that provides only a "single-tenant" approach to delivery of software services (i.e., a single instance of software serves a single customer, with the ability to customize the application features and functionality as required by the customer), and defined as such, the ASP service delivery model is quite different from both SaaS and cloud computing. Cloud computing, as with SaaS, is often described as including a "multi-tenant" approach to delivery of software services (i.e., a single instance of software serves multiple customers at the same time with each customer sharing hardware resources, but resulting in more limited customization options). A multi-tenant approach is used in cloud computing to improve resource utilization and scalability, with scalability being one of the most important distinguishing features of cloud computing and essential to making it possible for large-scale data centers to be able to cost-effectively provide computing resources to millions of users as a utility.

UTILITY BILLING FOR CLOUD COMPUTING

Cloud computing also may be distinguished from ASP with respect to billing. While there are cloud computing services that are billed on a subscription basis, cloud computing is also billed on a utility basis, such that the customer only pays for those resources used. Moreover, even if cloud computing services are billed on a subscription basis, usage above a set level usually triggers a utility billing model for such excess usage. Cloud computing solutions can provide customers the ability to request, and enable providers to deliver, only those resources needed, resulting in more efficient use of provider's IT resources (by avoiding over-utilization and under-utilization) and thereby enabling the provider to deliver services at a lower cost. If the provider passes such benefits through to the customer, then utility billing may be a more attractive option for customers.

Appendix C — Cloud Computing Contract Checklist

PRE-AGREEMENT VENDOR DUE DILIGENCE

- Questionnaire to vendors should include questions regarding:
  - Financial condition and corporate responsibility
  - Insurance
  - Existing service levels
  - Capacity
  - Use of subcontractors
  - Location of data
  - Security infrastructure and policies and procedures (administrative, technical, and physical security)
  - Disaster recovery and business continuity processes
  - Redundancy
  - Ability to comply with applicable laws

SERVICE AVAILABILITY

- Disaster recovery and business continuity
- Withholding of services
- Bankruptcy and financial wherewithal

SERVICE LEVELS

- Uptime
- Response time
- Simultaneous visitors
- Problem response and resolution
- Remedies

DATA SECURITY

- Business Associate Agreement
- Review of data security infrastructure and administrative, technical, and physical security policies and procedures
  - Physical site visit
  - SSAE 16
- Audits and inspections
- Disaster recovery and business continuity requirements
- Subcontracting arrangements
- Location of data
- Data redundancy
  - Frequency of data back-ups
  - Location of back-ups
- Breach notification
  - Procedures for investigation of breach
  - Content of notification of customer
  - Customer has sole control over notification of individuals and agencies
  - Reimbursement for costs and expenses
- Data ownership and use rights
  - Limitations on right to use data
- E-discovery
- Data conversion/data return
  - Format for return of data

INSURANCE

- Cyber-liability policy
- Technology errors and omissions
- Electronic and computer crime
- Unauthorized computer access
- Avoid only general liability policy

INDEMNIFICATION

- For breach of confidentiality and security requirements
- For infringement claims

LIMITATION OF LIABILITY

- Application to both parties
- Exclusions (from both consequential exclusion and cap on direct damages)
  - Breaches of confidentiality
  - Claims for which the vendor is insured
  - Indemnification obligations
  - Infringement of IP rights
  - Breach of advertising/publicity restrictions
- Overall liability cap as a multiple of fees

INTELLECTUAL PROPERTY

- Ownership of work product
- Use of ideas in services to competitors

WARRANTIES

- Data security
- Redundancy/disaster recovery/business continuity
- Performance in accordance with specifications
- Services provided timely and in compliance with best practices
- Provision of training as needed
- Compliance with laws (both the software and personnel)
- No sharing of client data
- Software will not infringe

- Software will not contain viruses
- No pending/threatened litigation
- Sufficient authority

LICENSE/ACCESS GRANT AND FEES

- Broad permitted use
- Avoid limitation to internal business purposes
- Application to affiliates, subsidiaries, outsourcers and others

IMPLEMENTATION

- Broad definition of services
- Description of any additional work to support functionalities

FEES

- Ability to add or remove resources
- Incremental and decremental use
- Identify all revenue streams

TERM

- Free ability to terminate
- Consider limited notice period
- Consider commitment period

ASSIGNMENT

- Ability to assign freely
- Assignee assumes responsibilities under the agreement

EXCLUSIVITY

- Consider service levels
- Appropriate exceptions
- Transition in anticipation of termination

ONGOING POST-EXECUTION PROVIDER ASSESSMENT

- Evaluation
- Data security audits

»

[1] Gartner Group, Gartner Says Worldwide Cloud Services Market to Surpass $68 Million in 2010 (June 22, 2010), available at *http://www.gartner.com/it/page.jsp?id=1389313*.

[2] From Tactic to Strategy:the CDW 2011 Cloud Computing Tracking Poll, CDW (2011), available at CIO Survey of HIT Adoption Trends (2012), http://webobjects.cdw.com/webobjects/media/pdf/Newsroom/CDW-Cloud-Tracking-Poll-Report-0511.pdf; see also Optum Institute for Sustainable Health, at http://institute.optum.com/research/featured-publications/cio-survey-of-hit-adoption-trends/~/media/OptumInstitute/Page_Elements/Articles/OPTUM_CIO_HIT_Survey_Feb2012.pdf.

[3] Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), codified at 42 U.S.C. §§ 300jj et seq.; §§ 17901 et seq.

[4] Cloud Computing in Healthcare, Cisco Knowledge Network (Sept. 16, 2011), available at http://www.cisco.com/web/IN/about/network/cloud_computing.html.

[5] Security Guidance for Critical Areas of Focus in Cloud Computing 3.0, Cloud Security Alliance (2011), available at https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf; see also Cloud Computing Synopsis and Recommendations, Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology (Pub. 800-146 (May 2012), available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075; Jansen, Wayne and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology (Pub. 800-144) (Dec. 2011), available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494.

[6] Jansen, Wayne and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology (Pub. 800-144) (Dec. 2011).

[7] Pub.L. 104-191, 110 Stat. 1936 (Aug. 21, 1996), implemented in regulations at 45 C.F.R. Parts 160 and 164. The Security Rule is set forth in 45 C.F.R. Subparts A and C, Breach Notification Rule in Subparts A and D, and the Privacy Rule in Subparts A and E.

[8] HIPAA Security Rule, 45 C.F.R. Subpart D.

[9] 15 United States Code (U.S.C.) § 6801 et seq.

[10] Payment Card Industry Security Standards, PCI Security Standards Council, available at https://www.pcisecuritystandards.org/documents/PCI%20SSC%20-%20Overview.pdf.

[11] Legal Resources — Statutes Relating to Consumer Protection Mission, Federal Trade Commission, available at http://ftc.gov/ogc/stat3.shtm.

[12] White, P. Jon and Daniel, Jodi, Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Law Requirements for Patient Permission to Disclose Health Information: Report on State Law Requirements for Patient Permission to Disclose Health Information.

[13] Security of Personal Information, N.R.S. § 603A; Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 C.M.R. § 17.00.

[14] Cal. Civil Code § 56.101.

[15] "Class Action Lawsuit Filed Against Stanford," Palo Alto Online News (Oct. 3, 2011); Health Data Privacy Driving New Type of Class Action Litigation, Kershaw, Cutter & Ratinoff LLP (April 10, 2012); KCR Files Complaint Against Health Net and IBM for Privacy Breach (April 19, 2011); "Sutter Health Data Breach Lawsuits Coordinated in Sacramento," Business Journal (Feb. 29, 2012); UCLA Hospitals Facing $16M Class Action for Stolen Patient Information, McDonald Hopkins LLC (Jan. 2012).

[16] Foley & Lardner LLP and Eversheds, International Security Breach Notification Survey (December 2011).

[17] Ponemon, Larry, Five Countries: Cost of Data Breach, Ponemon Institute (April 19, 2010), available at http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf.

[18] "EMC Spends $66 Million to Clean Up RSA SecureID Mess," Information Security (Aug. 3, 2011), available at http://www.infosecurity-magazine.com/view/19826/emc-spends-66-million-to-clean-up-rsa-secureid-mess/.

[19] The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security, American National Standards Institute, the Santa Fe Group, and Internet Security Alliance (2012), available at http://webstore.ansi.org/phi/.

[20] Under HIPAA, persons or entities who perform certain services for a covered entity and have access to a covered entity's PHI are considered business associates; see, 45 C.F.R. § 160.103; see, The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment, available at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/introduction.pdf*, for a discussion of health information exchanges as business associates.

[21] OCR, Frequently Asked Question, Is a software vendor a business associate of a covered entity? (Last updated: March 14, 2006), available at http://www.hhs.gov/hipaafaq/providers/business/256.html.

[22] CMS, Letter to all Medicare Advantage Organizations (MAO), Prescription Drug Plan (PDP) Sponsors, 1876 Cost Plans, and PACE organizations as applicable, Contract Year (CY) 2012 Medicare Advantage and Part D Readiness Checklist (Sept. 16, 2011).

[23] N.R.S. § 603A.030

[24] Cal. Civil Code § 56.06.

[25] TechRadar for Infrastructure & Operations Professionals: Cloud Computing, Q3 2009, Forrester Research, Inc. (Oct. 2, 2009), available at http://www.forrester.com/rb/Research/techradar%26trade%3B_for_infrastructure_%26_operations_professionals_cloud/q/id/54338/t/2.

[26] Gartner Highlights Five Attributes of Cloud Computing, Gartner, Inc. (June 23, 2009), at http://www.gartner.com/it/page.jsp?id=1035013.

[27] Defining "Cloud Services" and "Cloud Computing," IDC (Sept. 23, 2008), at http://blogs.idc.com/ie/?p=190.

[28] Mell, Peter and Timothy Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology (Pub. 800-145) (Sept., 2011), available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909616.

[29] Above the Clouds: A Berkeley View of Cloud Computing, EECS Department, University of California, Berkeley (Feb. 10, 2009), available at http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

[30] Cloud computing (last visited Sept. 21, 2012), at http://en.wikipedia.org/wiki/Cloud_computing.

*This white paper provides information about cloud computing issues. This information is not legal advice. Legal advice requires interaction between the attorney and the client, and the application of the law to an individual's or organization's specific circumstances. An organization should consult with an attorney if it requires advice pertaining to a particular situation, circumstance, or need, or in the event the organization has any questions regarding the application or use of any of the content.