

# Cloud Computing— Driving Security, Performance and Quality

Cloud computing is the latest in a set of outsourced IT paradigms that the healthcare industry has begun to embrace, particularly over the past decade.

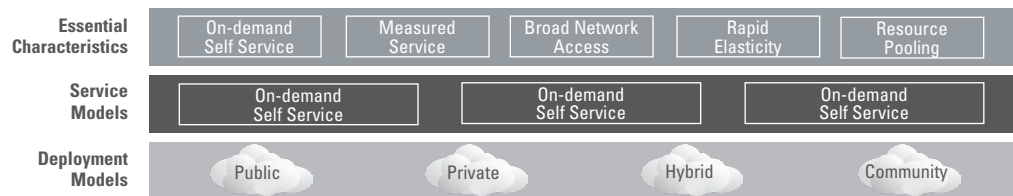
Ubiquitous adoption of Internet technology has swung the pendulum of enterprise software design and usage back to the client-server model first introduced by terminals connected to mainframes half a century ago. What has shifted quite a bit from that era though, is the business and physical relationship between consumers and providers of information services, data, hardware and software—with outsourcing as a key business driver. This new business and technology framework drives specific regulatory and IT-security considerations that need to be correctly addressed, but also gives software providers such as Medidata the opportunity to offer customers products and services of a much higher quality and integrity than previously available to the industry.

## Cloud Computing Demystified

The creation of Internet technology-based information services in our industry requires specific clinical development domain expertise, software development and maintenance skills, and server, data storage and Internet Protocol (IP) communication technology know-how. Just as many R&D divisions at healthcare and life sciences companies have moved away from custom application development to reliance on third-party software over the past decade, they are now questioning whether internally hosting and servicing these applications models are core, competitive capabilities. Increasingly, there is a higher comfort level in outsourcing software development, maintenance and data hosting to Software-as-a-Service (SaaS) providers that demonstrate the appropriate stability, capabilities and experience.

SaaS is just one of the more familiar flavors of cloud-based services. In general, cloud computing is defined as 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. As much as biopharmaceutical companies and contract research organizations (CROs) have increasingly entrusted the development, delivery and maintenance of their clinical development software and data to SaaS providers, all parties involved have recently begun to explore outsourcing some of their required computing infrastructure (web and applications servers, databases, etc.) to highly proficient and efficient Infrastructure-as-a-Service (IaaS) providers such as Amazon Web Services (AWS).

FIGURE 1:  
VISUAL MODEL OF NIST'S  
WORKING DEFINITION OF  
CLOUD COMPUTING



<sup>1</sup> National Institute of Standards and Technology, NIST Definition of Cloud Computing v15, 2009.

Made possible by “virtualization” technology and increasingly high-speed Internet bandwidth, cloud IaaS is a relatively new approach, whereby the actual computing resources (server software, operating systems and physical infrastructure) are geographically disparate, “rented on-demand,” shared by multiple “tenants” and communicated with over the Internet using web-service-based application programming interfaces (APIs). Consumption is typically billed using utility or subscription-based models. Much of this description, at first glance, might seem applicable to more traditional leased data center arrangements. However, the combination of virtually unlimited infrastructure resources available practically instantaneously (compare a couple of months necessary to provision a traditional server with a couple of minutes for a cloud-based server), configured via a standard API and billed like a utility (e.g., by the hour) creates some important, very positive game-changers with respect to hosted software testing, validation and performance, which will be described later on in greater detail.

### Extra Diligence is Required—And Rewarded

Multiple privacy and confidentiality issues affect the regulatory requirements of cloud computing participants. For example, the location of information in the cloud affects the privacy and confidentiality of information and the obligations of data processors and controllers. A customer’s privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider. Among the questions to be asked are:

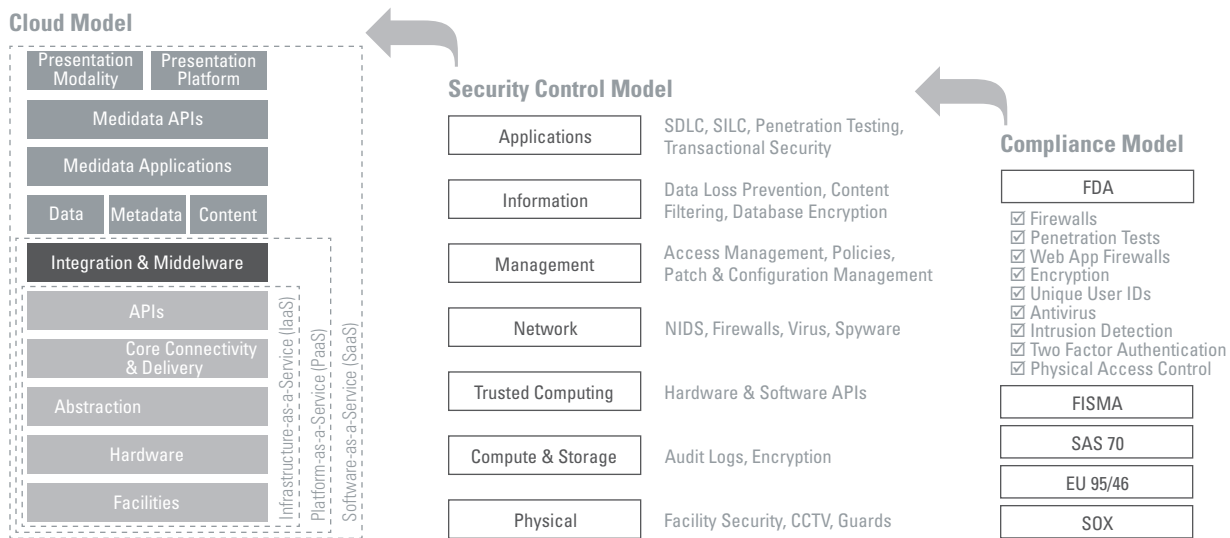
- How well is the discovery process supported in a legal proceeding?
- Can information derived by the cloud provider violate data privacy laws or original owner rights?
- Which specific countries could the cloud-stored information physically end up in and what are the applicable laws where the physical machine resides?

Medidata carefully and diligently considered these and other issues in preparation for transition of some its software and data to a cloud environment. The result has been an information security architecture that has positioned Medidata to prescriptively and repeatedly demonstrate compliance with a cornucopia of international regulations, including in recent inspections from the UK’s Medicines and Healthcare products Regulatory Agency (MHRA) and a Federal Information Systems Management Act (FISMA) evaluation.

Prior to evaluating potential cloud service providers, high-level requirements such as data integrity, confidentiality and authenticity, as provided by relevant regulations (including FDA 21 CFR, FISMA, SAS 70 and EU95/46), needed to be mapped to a unified Security Control Model. Figure 2, adapted from Cloud Security Alliance’s Security Guidance, shows an example of how a cloud service mapping can be compared against a catalog of compensating controls to determine which controls exist and which do not, as provided by the consumer, the cloud service provider or a third party. By reviewing the security policies of a number of candidate IaaS providers were then reviewed for sufficient compliance with the security model and identification of gaps, Medidata was able to formulate and adopt best practices that meet the unique needs of our industry in a cloud environment, including:

- Encrypting “at-rest” any customer data that would be deployed into a public cloud in addition to the encryption of API communications and data in transit,
- Deploying host-based firewalls on all servers in addition to the cloud provider’s firewall—both adding an independent, internally-controlled and additional layer of protection irrespective of the cloud provider’s measures and the physical location and disposition of the data, and
- Ensuring that cloud servers would be provisioned with only Medidata software and data, mitigating the highly unlikely yet potential risks of multi-tenancy.

[ FIGURE 2: MAPPING THE CLOUD MODEL TO THE SECURITY CONTROL AND COMPLIANCE MODEL<sup>2</sup> ]



Physical inspection of a cloud provider’s facilities, including meetings with key facility personnel, provides the opportunity to observe physical evidence of the service provider’s security policy implementation, to better understand how security procedures would be enforced and to get a sense for how the facility operates and withstands adverse events. After satisfactorily concluding this portion of the security assessment, Medidata deploys a fully functional software environment with test data on the cloud provider’s infrastructure and a week-long set of penetration tests by an independent third party are conducted to ensure that it is neither possible to “break-in” (breach the integrity or the confidentiality of data as an unauthorized user) nor “break-out” (cause similar harm as a user with some measure of authorization, i.e., given a username and password). Only upon successful completion of this final phase is the green light given to leverage the cloud provider’s infrastructure for production software services.

## Ultimate Software Quality and Infinite Scalability

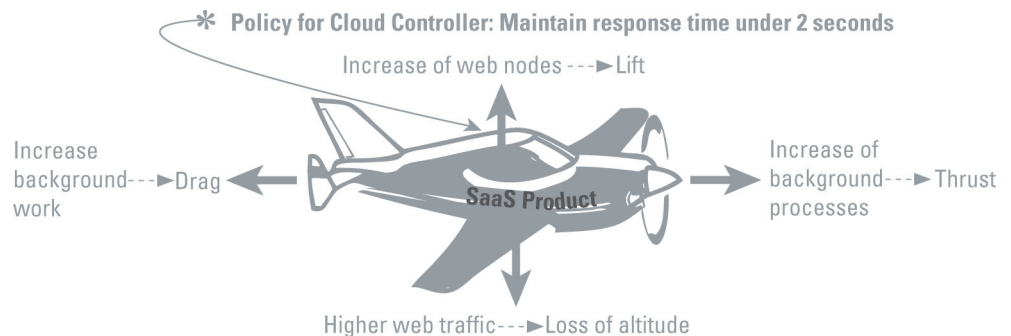
As mentioned earlier, cloud computing creates some game-changing opportunities with respect to software quality and performance. Appreciating the impact on quality starts by understanding that despite the best of intentions, software development has, until recently, suffered from the disparity between the infrastructure used to develop and test applications and the production environment used to run them. Rarely has it been economically viable, practically feasible or worth the wait for developers and testers to provision a hosting environment (server, security and storage hardware, operating systems, server software, etc.) of the same scale and with the same configuration effort as for those used in ongoing operations in support of customers. As a result, software quality has suffered and testing and validation of production software has been resource- and time-intensive. On-demand cloud computing, however, changes all that.

Medidata can now leverage IaaS to fire up full-scale hosting environments identical to those used in production for a few hours or days of development or testing, and just as quickly decommission these environments at a fraction of the time or cost of previous infrastructure provisioning models. This not only eliminates resource bottlenecks and quality issues stemming from environment disparity, it makes executing real-world performance tests completely feasible. Even more importantly, the use of cloud infrastructure takes the delivery of high performance software services to an unprecedented level.

<sup>2</sup> Adapted from the Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance, 2009

Standardized cloud infrastructure APIs have fueled the development of open source, domain-specific languages (e.g., Opscode Chef) to control entire hosted environments via standardized code. It is now completely practical to designate high-level IT policies whose business logic is codified by software using these languages, e.g., “self-healing” processes whereby all infrastructure status metrics are constantly monitored and any element failure is addressed by immediately firing up a replacement and provisioning it appropriately in minutes. Likewise, any spike in utilization can be nearly instantaneously addressed with an increase in hosting infrastructure applied to the delivery of a particular service, to be decommissioned just as fast when demand drops. In essence, IaaS enables cost-effective, instant, “infinite scalability” to support the most demanding of clinical research operations and creates a granularity of performance control akin in many ways to that used to fly an airplane, as depicted in the figure below.

FIGURE 3:  
GRANULAR CONTROL OF SaaS  
PERFORMANCE POLICIES USING  
“INFRASTRUCTURE-AS-CODE”



Provisioning and controlling entire infrastructure environments and individual elements via “Infrastructure-as-Code” has tremendous value in ensuring consistent quality and demonstrated validation of the complete application stack, from soup to nuts. It also allows the entire operation of a software provider such as Medidata to be easily reconstructed and brought live in a matter of hours solely from a back-up of the data, application software components and the infrastructure code files—providing customers with an unprecedented level of confidence with respect to disaster recovery, and Medidata with complete freedom to select ad hoc an IaaS provider that meets the right business and quality requirements at any given time.

## About Medidata Solutions

Medidata Solutions is a leading global provider of SaaS-based clinical development solutions that enhance the efficiency of customers’ clinical trials. For over 10 years, Medidata has consistently brought next-generation innovation to the life science industry to lower the total cost of clinical development. Medidata’s advanced solutions address key functions throughout the clinical development process including protocol development (Medidata Designer®), trial planning and management (Medidata Grants Manager®, Medidata CRO Contractor®), clinical portal (iMedidata™), randomization and trial supply management (Medidata Balance™), monitoring (Medidata Rave Monitor, Medidata Rave Targeted SDV), SAE capture (Medidata Rave Safety Gateway) and clinical data capture, management and reporting (Medidata Rave®).

mdsol.com | info@mdsol.com | +1 877 511 4200



Trademarks are the property of their respective owners.  
Copyright © Medidata Solutions, Inc. 2010 09/10

Technology for a healthy world.®

CLINICAL PORTAL | PROTOCOL DEVELOPMENT | TRIAL PLANNING & MANAGEMENT | MONITORING  
DATA CAPTURE & MANAGEMENT | RANDOMIZATION & TRIAL SUPPLY MANAGEMENT | CODING | SAE CAPTURE