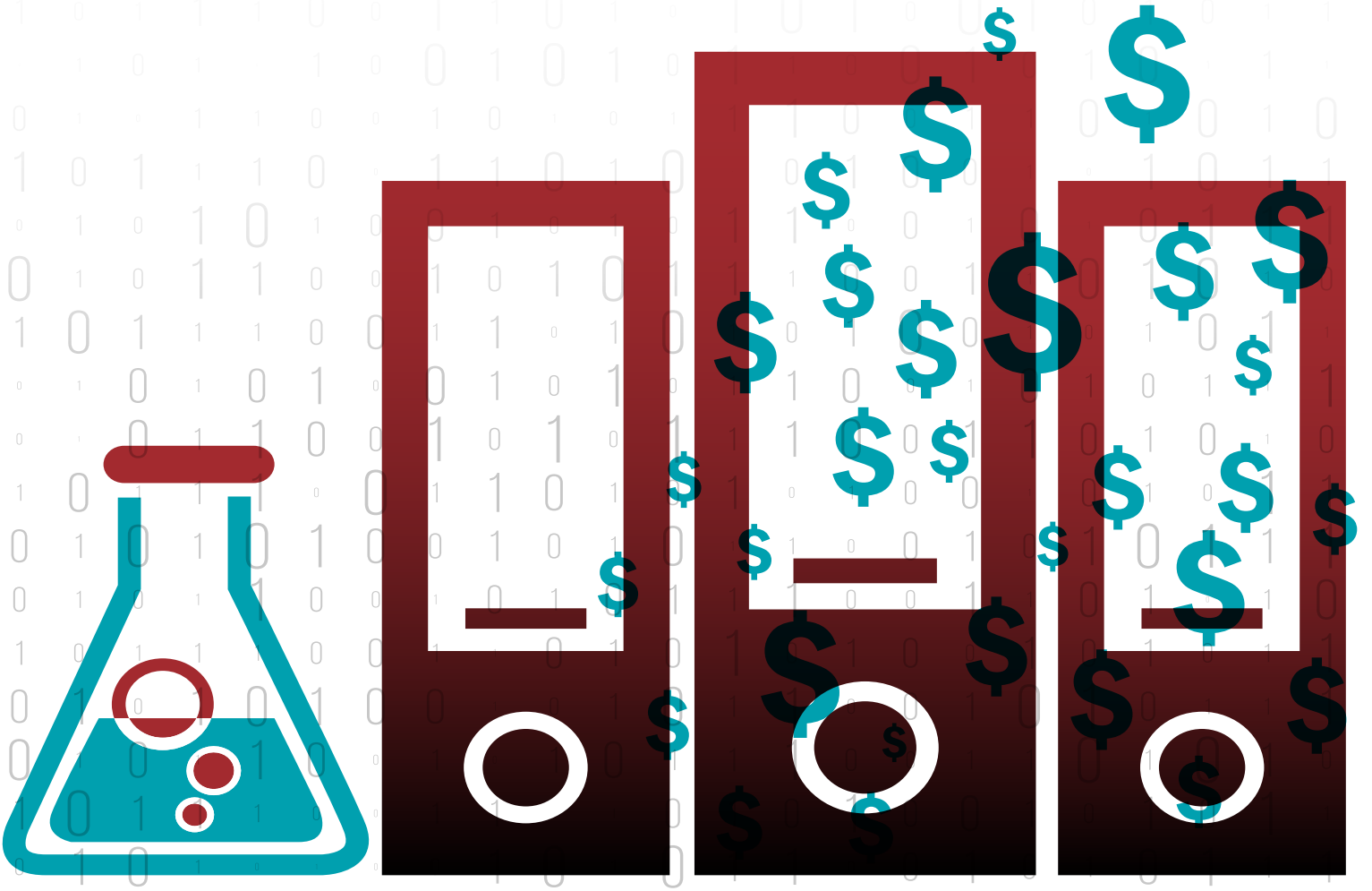
Breaking Through the Cloud:

A LABORATORY GUIDE TO CLOUD COMPUTING

Seeing these IT issues/challenges in *your* laboratory?

- Balancing the cost of purchasing, housing, implementing and maintaining servers with other laboratory costs.
- Processing huge amounts of data requires higher orders of computing ability, expertise to implement intricate software to translate complex mathematical models into functional algorithms and vast amounts of secure, high-speed storage.
- The potential for accidental or intentional misuse of data stored on physical, in-house servers.
- Difficulty finding central information technology (IT) staff that can be committed to learning business processes due to IT consolidation.
- Competition for data exchange resources—which require specialized programming and developer expertise in laboratory processes and testing—is difficult and often costly.
- Lack of interoperability between various systems to collect and record data, including laboratory information systems management systems (LIMS), Excel or Access spreadsheets and homegrown systems, which slow information sharing within the laboratory and with external partners.

Cloud computing may be able to help.



what is cloud computing?

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. For some companies/institutions, it offsets the need to store the data locally, potentially saving costs.

You are probably already using cloud computing in your organization or in your everyday life if you use systems like Google Apps or Office 365, two of the most common cloud computing technologies on the market.

Are cloud computing systems all the same?

The two main cloud computing solutions, "Infrastructure as a Service" (IaaS) and "Software as a Service" (SaaS), allow an organization to focus on its core business needs, rather than investing effort in maintaining systems. While IaaS gives the most control, it requires more technical expertise to operate.

Infrastructure as a Service (IaaS)

- Provides virtual computer resources to build a technical environment or platform. This eliminates the need to maintain physical infrastructure and data centers.
- Places responsibility for auditing, encryption and other security measures primarily with the customer.

Software as a Service (SaaS)

- Allows a business to connect to and access an application over the Internet. One example would be Microsoft Office Online, an online version of the office suite in the form of web applications.
- Places responsibility for security primarily with the provider. For example, under BaseSpace Clarity LIMS, the provider handles password controls, data backups, encryption and other security controls.

IaaS/SaaS Cloud Service Providers

The three cloud service providers (CSPs) have similar offerings, but differ in pricing structures. Select a CSP with the right tools and options to support your laboratory.

Amazon Web Services (AWS)
Amazon Web Services offers a number of IaaS solutions, including Elastic Cloud Compute (EC2), which provides resizable computer capacity in the cloud.

Microsoft Azure
The Microsoft Azure Platform is used to power SaaS solutions like Microsoft Office 365. Office 365 includes SharePoint Online, Exchange Online and Lync Online.

Google Cloud Platform
The Google Cloud Platform powers Google Compute Engine, which delivers virtual machines similar to AWS EC2. Compute Engine is one of many IaaS components of Cloud Platform.

"**ONE OF THE BIGGEST BENEFITS** of our project has been the ability to on-board the labs quickly. We saved at least 1.5 years on the entire project (for four labs) because the infrastructure is cloud-based and therefore centralized and everyone has to use the same process."

Elizabeth Neuhaus, PhD
Associate Director for Informatics
Influenza Division, CDC

why use cloud technology?

Cost Savings

- Scale technical capabilities based on fluctuations in demand or workload for potential cost savings. (In a situation with fluctuations in workload, cloud computing can potentially render cost savings even if the constant cost fluctuates over time based on activity. However, there are still costs associated with licensing and actual manpower needed to manage the environments with IT skills.)
- Minimize investment in launch infrastructure to eliminate the need for upfront capital expenses.

Agility

- Rapidly provision resources leveraging cloud computing's elastic model.
- Adapt to growth and change without changes to technical hardware or assets.

Control Inheritance

- Inherit some security control protection and compliance from existing cloud service providers
- Perform varying levels of management and upgrades depending on cloud computing category

High Availability

- Maintain a presence in multiple regions of the world.

how is data kept safe?

Cloud computing can deliver better security services than many organizations could provide on their own. CSPs can offer advanced security and privacy facilities that leverage their scale and skills at automating infrastructure management tasks. This is a boon to customers who have few skilled security personnel.

Be sure to understand a CSP's security requirements before you select a system, especially if you are responsible for protected health information (PHI).

CSPs observe the following protocols to mitigate security risks:

Shared vs. Dedicated Tenancy: Multiple cloud customer's machines may reside on the same server instance although systems storing public health information should have dedicated instances.*

Business Associates Agreements: An agreement between the customer, provider and technical vendors must be in place when working with HIPAA-eligible data.

Auditing: CSPs must keep detailed activity logs and reports and continually monitor access. These reports are tracked, logged and stored in a central location for extended periods of time for auditing purposes. Activity logs should identify who accessed the data and from where and how the data may have been altered.

Risk Analysis: CSPs and customers should both conduct independent assessments of potential risks and vulnerabilities to the confidentiality, integrity and availability of PHI held by the organization.

**Ask your CSP how they ensure the security of public health laboratory data.*

"CLOUD COMPUTING IS HERE. We know the benefits of engaging in the cloud but it is our responsibility to be educated on how to properly use cloud resources, how to manage costs and most importantly, how to assure the cloud environment is secure. "

Eduardo Gonzalez
Chief Executive Officer, UberOps

how do I engage or evaluate a cloud service?

1. **Consider filling out the APHL Self-Assessment Tool**. The tool allows public health laboratories to assess strengths and gaps in informatics capability by addressing 19 critical operational areas. It charts data longitudinally, enabling laboratories to measure growth and leverage results to advocate effectively for their needs. The tool also offers a suite of data visualization tools that display assessment data graphically and segmented in multiple ways. This exercise will enable an institution to understand their informatics strengths and gaps as they think about using a cloud service

2. **Engage IT staff** to see if cloud computing is possible, or if there are agreements in place for specific CSPs. For example, it is important to distinguish that a LIMS product running on a cloud system is very different than a LIMS deployed on servers that are purchased and maintained by an organization.

3. **Engage security staff** to see if cloud computing is possible, given current security requirements.

4. **Develop a project plan** listing goals, objectives, benefits, etc. As the plan is developed, consider what would be stored in the cloud, as not everything belongs there. Consider latency issues. For example, most instrument control computing systems should not be in the cloud. However, they can be designed to share data in network storage systems and/or be integrated with cloud-based LIMS through various communication paths.

5. **Complete an alternatives analysis** (a comparison of operational effectiveness, cost, and risks) on multiple cloud services. Data security should also be discussed in the context of this analysis.

For more information on cloud computing, visit www.aphl.org/cloudcomputing

"**USING THE AIMS CLOUD** would definitely be a viable option for IaaS for next generation sequencing (NGS) for sentinel public health laboratories, and it has been proven effective for well over a year now."

Elizabeth Neuhaus, PhD
Associate Director for Informatics
Influenza Division, CDC

REFERENCES: Cloud Standards Customer Council. Security for Cloud Computing: Ten Steps to Ensure Success, Version 2.0. March, 2015
Available at *http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf*

ASSOCIATION OF PUBLIC HEALTH LABORATORIES

The Association of Public Health Laboratories (APHL) works to strengthen laboratory systems serving the public's health in the US and globally. APHL's member laboratories protect the public's health by monitoring and detecting infectious and foodborne diseases, environmental contaminants, terrorist agents, genetic disorders in newborns and other diverse health threats.

This publication was 100% funded with federal funds from a federal program of $674,993. This publication was supported by Cooperative Agreement # NU60OE000103 funded by the US Centers for Disease Control and Prevention (CDC). Its contents are solely the responsibility of the authors and do not necessarily represent the official views of CDC or the Department of Health and Human Services.

APHL®

8515 Georgia Avenue, Suite 700
Silver Spring, MD 20910
Phone: 240.485.2745
Fax: 240.485.2700
Web: www.aphl.org

© Copyright 2017, Association of Public Health Laboratories. All Rights Reserved.