Uploaded to the VFC Website
▶▶   May 2015   ◀◀

This Document has been provided to you courtesy of Veterans-For-Change!

Feel free to pass to any veteran who might be able to use this information!

For thousands more files like this and hundreds of links to useful information, and hundreds of "Frequently Asked Questions, please go to:

Veterans-For-Change

If Veterans don't help Veterans, who will?

Note: VFC is not liable for source information in this document, it is merely provided as a courtesy to our members & subscribers.

Riverside County, California

THE BRAVE NEW WORLD
OF CONSOLIDATED AND SHARED IT SERVICES:
A Guide for Laboratories

APHL ASSOCIATION OF
PUBLIC HEALTH LABORATORIES

APRIL 2011
AUTHORS: APHL INFORMATICS COMMITTEE

EXECUTIVE SUMMARY

Recent advances in laboratory instrumentation and the importance of electronic data exchange have shifted isolated laboratory processes to a collaborative continuum of client services dependent not only on good laboratory practices, but on the flexibility of Information Technology (IT) services supporting these practices. Many government jurisdictions (state governments in particular) are moving their IT provision models to consolidated/centralized services or shared services, with potentially great impact on public health and other governmental laboratories. Because these laboratories exist in states, cities and counties with multiple mandates and IT needs, each faces unique IT challenges. Like state laboratories, shared IT service arrangements can take many forms. This paper describes the difference between consolidated and shared IT services models, drivers of IT consolidation, possible impacts on the laboratory and factors to consider when negotiating with centralized IT leaders, with the ultimate goal being to optimize operational efficiency to benefit laboratories and their customers. There is a particular focus on describing the totality of the laboratory IT infrastructure (which is more than just the laboratory information management system) and how best to approach negotiations involving the two major tools for consolidated/shared services management: the memorandum of understanding (MOU) and service level agreement (SLA).

1. BACKGROUND

This paper was developed by APHL's Informatics Committee to inform leaders of public health, agricultural and environmental testing laboratories about the possible benefits and drawbacks of various Information Technology (IT) service models. For some years, Informatics Committee members have been active observers and participants in a nationwide trend toward the centralization of information technology services at the state or local government level. They created this document as a guide to understanding the different approaches to laboratory information management IT services.

On the one hand, IT centralization may increase efficiency in some areas, reduce costs and enable the laboratory to access equipment or services that were previously *unaffordable. For example:

○ *In one state, implementation of an active directory service for user accounts resulted in robust intranet storage supported on two separate portions of the network grid, achieving zero down time and zero data loss.*

○ *In another example, consolidation of desktop support enabled a failed operating system to be restored in just a few hours.*

But, on the other hand, poor implementation choices, insufficient communication among partners and weak management structures can increase costs and have disastrous effects on a laboratory's ability to fulfill its mission.

○ *One state PHL received federal funds to procure 50 badly needed desktop computers. Soon after the purchase and installation, the state's IT center mandated that all desktop computers conform to a new standard; one with minor variations from the newly purchased computers. The state PHL was required to replace all 50 computers.*

○ *In another state, the public health laboratory was unable to provide emergency desktop computers to regional laboratories during the 2009 Influenza*

A H1N1 pandemic because of a lengthy delay in authorizing the purchase.

○ *In yet another state, laboratory staffs were unable to print essential reports when a shared server— maintained off-site from the laboratory—went down. Since laboratory staff did not have administrative rights to the server, they were dependent on central IT staff to correct the problem.*

An informal poll by the APHL Informatics Committee of several PHLs,[1] with varying degrees of IT consolidation, reveals significant concerns about IT consolidation among laboratory leaders:

• Excessive and extremely rigid bureaucracy;

• A lengthy decision-making process that could compromise emergency response;

• Inadequate laboratory representation on decision-making bodies whose decrees have wide-ranging impact on the laboratory;

• Insufficient laboratory input into the design and management of laboratory data systems and a crucial lack of technical understanding of laboratory operations among those who do have significant input;

• The possibility that high IT infrastructure and administration costs may not be recouped through the limited revenue streams available to the laboratory;

• The high costs of IT that need to be included in grant applications compromises grant awards and the ability to complete awarded grants. Also, the budget cycle for IT funding is not meshed with laboratory grant funding cycles.

While laboratory leaders cannot control all of these factors, they can better equip themselves to advocate effectively for their organization to maximize the advantages of any IT service model.

....
(1)   Feedback from the APHL Informatics Committee, input provided at a 2010 meeting.

2. INTRODUCTION

Once thought of as a support function, the delivery of laboratory IT services has now evolved to the point where electronic recordkeeping and automated data management are mission-critical components of public laboratory operations.

Yet, while laboratories may once have had complete control over essential informatics activities, more often than not, this is not the case today. To increase efficiencies and cost-savings, many states and other jurisdictions are moving to either consolidated (i.e., centralized) IT services or shared services (a hybrid model with aspects of centralization and decentralization). In fact, the National Association of State Chief Information Officers (NASCIO) reports that consolidation of IT services is the number one priority for state chief information officers (CIOs) in 2011, followed by cost control and healthcare IT solutions.[2]

Consolidated or shared IT services have potential to reduce costs and achieve certain benefits, but they also pose new challenges for laboratory leaders.

IT investments are both costly and consequential to laboratories. Spending on IT equipment, services and laboratory information management systems (LIMS) are among the largest expenditures a laboratory makes. A 2004 study documented in a white paper, *Batteries Not Included*, estimated the first-year LIMS cost—including acquisition, implementation and maintenance—at anywhere from $275,000 to $1.5 million, depending on laboratory size.[3] A more recent, unpublished APHL study shows these first-year costs can now reach up to $3 million for a commercial, off-the-shelf LIMS with multiple modules.[4] While critically

important, the LIMS represents just one piece of the laboratory IT infrastructure.

Inappropriate IT resource management decisions not only increase the likelihood of IT failures—and the massive disruptions these may cause—but can expose the laboratory to potential legal liability; for example, if private information is not adequately safeguarded or if laboratory data is misdirected.

> "The failure of a LIMS to provide rapid newborn screening data can result in death or lifelong morbidity."
>
> **Willie Andrews, BS, MT(ASCP)**
> **Laboratory Operations Director**
> **VA Division of Consolidated Laboratory Services**

No one expects the laboratory director to write code. But, in jurisdictions where centralized or shared IT services are in use or under consideration, it is imperative that laboratory leaders have a high-level grasp of IT service options and associated costs, understand the importance of cost-effective implementation, maintain a working relationship with the CIO and IT managers, and be able to communicate the information management activities and technologies needed to support the laboratory.

(2)   NASCIO. State CIO Top Ten Policy and Technology Priorities for 2011.
        October 2010. www.nascio.org/publications/. Last accessed February 15, 2011.

(3)   Public Health Informatics Institute and APHL. *Batteries Not Included.*
        April 2004. http://www.aphl.org/aphlprograms/informatics/Documents/Batteries.pdf.
        Last accessed February 15, 2011.

(4)   *Moving Toward Interoperability: Laboratory Information Management Systems (LIMS) and Meaningful Use of Laboratory Data* whitepaper, prepared for the Association of Public Health Laboratories by Booz Allen Hamilton, May 7, 2010.

2. INTRODUCTION (CONTINUED)

Given good fiscal responsibility by IT managers, steps to consolidate IT resources can preserve and improve customer satisfaction. One such step, data governance (an emerging discipline focused on the formal management of data assets throughout an organization), relies on continuous business analysis to improve IT operations. Both laboratory science and informatics are fields in which change is expected. Just as assays change more quickly than testing platforms, data systems analysis models change more quickly than installed software.

This paper, along with any future companion references, offers recommendations for strategic planning with information service partners, specifically:

○ **Communication guidance** to enable laboratory leaders to convey the unique business needs of the laboratory in terms meaningful to CIOs, and to ask appropriate questions regarding the benefits and risks of a consolidated or shared IT services environment.

○ **Operational guidance** so laboratory leaders (a) can distinguish among various models for implementing consolidated/shared IT services, (b) understand the most important terms and provisions appearing in memoranda of understanding and other operational agreements, and (c) are familiar with the organizational and operational adjustments that may be needed to effectively employ consolidated/shared IT services.

The ultimate goal is to enable laboratory leaders to advocate effectively for IT solutions that best support their organization's customer-focused, public health mission.

3. CONSOLIDATED IT AND SHARED SERVICES

IT resources are assets that include far more than hardware and software. Most information technologies require significant support functions and services to make them useful.

NASCIO is the primary voice of state CIOs and an important partner whose support can strengthen the laboratory's own voice when states or other jurisdictions debate IT options. The association has published an issue brief on consolidated and shared IT services models, and its terminology is used throughout this paper.[5] NASCIO defines three major models for the organization and delivery of these IT resources to end users: (1) centralized or consolidated systems, (2) shared, 'hybrid,' systems, and (3) distributed, decentralized IT systems.[6]

Even NASCIO acknowledges that the terms "consolidation" and "shared services" are sometimes used "almost interchangeably." In fact, the NASCIO association describes a continuum of IT service arrangements with variables at each level that may be influenced by the political situation within a jurisdiction. From their perspective, shared services may be one step on the road toward consolidation, or consolidation might be viewed as a case of all-inclusive shared services.

NASCIO notes, however, that "although they seem to be two flavors of similar endeavors [consolidated and shared services] they are nevertheless different. "Basic definitions following.[7]

3.1 Consolidated or Centralized IT Services Model

According to NASCIO, a consolidated or centralized IT model "focuses on how states organize the delivery of IT services by combining existing organizations, services or IT applications into a single operation, typically mandated by executive order or statute." In extreme cases of IT consolidation, the laboratory would have little access and no dedicated resources to manage its computers, printers and associated LIMS hardware and software.

> "Within a fullly consolidated IT model, there is often compulsory participation and less direct dialogue among partners."

Typically, once a transition to a consolidated IT model has begun, budgetary and policy constraints make it difficult for any one agency or administrative unit to opt out. The new *modus operandi* may even involve the use of private, third-party vendors for IT support, placing these services even further from the laboratory and possibly limiting support activities to a pre-selected menu of services. In sum, within a fully consolidated IT model, there is often compulsory participation and less direct dialogue among partners.

---

(5)   NASCIO. *IT Consolidation and Shared Services: States Seeking Economies of Scale.* March 2006. http://www.nascio.org/publications/documents/NASCIO-Con_and_SS_Issue_Brief_0306.pdf. Last accessed April 14, 2011.

(6)   While rarer, successful decentralized models exist within the public health laboratory community. This distribution model is not a focus of this paper.

(7)   These definitions were derived from the work of NASCIO's 2004-05 IT Governance & Service Reform Committee and NASCIO's 2005-06 Enterprise Infrastructure & Services Committee.

3. CONSOLIDATED IT AND SHARED SERVICES (CONTINUED)

3.2 Shared IT Services Model

NASCIO describes the shared IT services model as one that "focuses on the delivery of a particular service or services in the most efficient and effective manner as a way of gaining economies of scale and other benefits. The centralization of specific IT activities that function as everyone's vendor of choice usually implies voluntary or consensus participation by the parties managed through the use of memoranda of understanding (MOUs) and more formal service level agreements (SLAs)." Shared or 'hybrid' service arrangements include some consolidated IT functions and some decentralized or distributed functions.

In a shared services system, individual departments have more say in their IT operations. Organization-wide or 'enterprise' functions are performed by a central IT unit. Shared functions might include data storage, network and infrastructure operations, e-mail, procurement, standard architecture and development of software applications for use across departments. Departmental functions, on the other hand, include development of department-specific software (up to a certain size) and planning for the department's IT needs. All of these activities must comply with common standards, overseen by central IT managers and a governance committee.

Needless to say, a shared services model works best within a culture of sharing; that is, when there is cooperation and collaborative management (i.e., implied partnership) between IT managers and department leaders. Actual shared services are then selected through a consensus-building process, focusing on 'best of breed' options.

In July 2005, Computer Science Corporation developed an information technology strategy for the Massachusetts Department of Public Health indicating that many department subsections—such as the laboratory—have self-contained functionality. This assessment led to a blend of centralized and decentralized IT elements—essentially, a structural hybrid or shared services model. In such a strategy, centralized activities should include the provision of a stable computing environment at the hardware, operating system, network and shared applications levels; similar to providing an organization with the utilities needed to power core business activities. Since the point of a well constructed shared services model is to focus on the common elements of the IT infrastructure, LIMS administration would be a subsection function.

3.3 Drivers of IT Consolidation

Now, more than ever, state and local government strategic plans list IT consolidation as a goal. These plans may bethe result of executive orders, legislative directives or recommendations from an audit agency. The 79th Texas Legislature, for example, mandated a new direction for technology management within the state government through the passage of House Bill 1516, signed into law September 2005. The law creates "statewide technology centers," approves the use of "joint information resources managers" and requires the use of "state commodity hardware configurations" for certain activities; all of which accelerate IT consolidation.[8] At least ten other states have similar laws in effect.[9]

---

(8) H.B. No. 1516, passed by the 79th Texas Legislature, September 2005, http://www.legis.state.tx.us/tlodocs/79R/billtext/html/HB01516F.HTM. Last accessed April 30, 2011.

(9) NASCIO Survey on IT Consolidation & Shared Services In The States: A National Assessment. May 2006. http://www.nascio.org/publications/surveys.cfm. Last accessed February 15, 2011.

3. CONSOLIDATED IT AND SHARED SERVICES (CONTINUED)

Of 35 state CIOs responding to a 2005 NASCIO survey, 33 reported planned, ongoing or completed projects to consolidate specific IT services, mostly in cooperation with or at the behest of the state legislature or governor's office.[10]

One factor driving IT consolidation is **technology** itself. Redundant disk arrays permit the central storage and management of hundreds of terabytes of information at relatively low cost. Server virtualization products enable a single computer to run multiple software products, each designed for a different operating system. And advances in network interface cards and fiber optics increase wide area network speed and reliability.

A second major driving force is **cost-savings**. Eliminating redundant hardware, software and support services can reduce costs significantly, especially operating costs. Moreover, a greater reliance on commodity products, in place of specialty products, results in additional cost savings. (For example, laboratory leaders know firsthand that incorporating standardized LIMS components, where possible, is less expensive than developing custom software for every LIMS application. It can also result in a higher quality product.) Other driving forces include:

- **Simplified maintenance** and support services due to standardization of the IT infrastructure.

- **Enhanced security management** and compliance with state and federal mandates.[11]

- Greater **interoperability** across computer systems due to the use of common technology and common data standards.

- Compliance with recommended **best practices** for IT technology management.

- Increased **purchasing power** due to the consolidation of retail orders and the use of fewer vendors.

....

(10) Ibid.

(11) "The key element to managing an information security program is information – about agencies' security postures, activities and threats. Agencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way." - Vivek Kundra, named Federal Chief Information Officer (CIO) by President Barack Obama at the White House on March 5, 2009.

4. A USER'S GUIDE TO SUCCESSFUL IT SERVICES NEGOTIATIONS

Consolidated and shared IT services are now a fact of life for many laboratories, and if not, may soon be. As such, laboratory directors must be prepared to advocate on behalf of the laboratory's IT needs. The following sections describe:

1. The totality of the IT infrastructure that must be considered in any service negotiation;

2. The two major tools used to negotiate, document and assure accountability for the delivery of IT services.

4.1 Understanding the Laboratory IT Infrastructure Framework

The LIMS familiar to virtually all governmental laboratory directors is the most visible component of the laboratory's IT infrastructure; the proverbial 'tip of the iceberg.' To be sure, technologies such as the LIMS and associated hardware and software are critical assets. However, the larger IT infrastructure also includes:
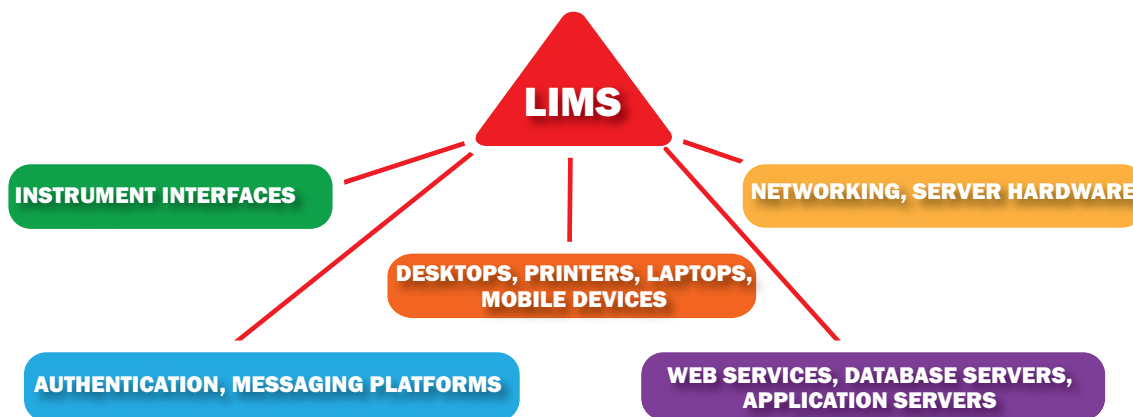
○ **Governance functions**, such as contract oversight, budgeting for IT products and services, policymaking and other management activities.

○ **Technical support**, including software customization, staff training, trouble-shooting and other activities to implement commercial technologies and otherwise assist end-users.

Understanding each of these components—along with associated costs, risks, metrics and implementation strategies—is key to productive negotiations with IT leaders.

4.1.1 IT Technologies Necessary for Successful Laboratory Operations

Modern governmental laboratories require a variety of IT technologies. Some of these, such as laptop computers and budgeting software, will be familiar to IT leaders outside the laboratory. Others, such as computerized analytical instruments and instrument interfaces, are specific to the laboratory and will be unfamiliar to most IT professionals. These technologies and associated service needs must be explicitly discussed. Table 1 (page 10) provides a summary of essential laboratory IT technologies; Figure 1 (below) shows how these interrelate.

FIGURE 1. MULTI-TIERED, PHYSICAL LABORATORY IT INFRASTRUCTURE

TABLE 1. IT TECHNOLOGIES NECESSARY FOR SUCCESSFUL LABORATORY OPERATIONS	
✓	
	Server Hardware
	Authentication and Authorization Technologies
	Web Platforms
	Communications Platforms
	Networking Hardware and Software
	Database Platforms
	Integration Brokers
	Desktop and Laptop Computers
	Printers, Copiers
	Mobile Devices (e.g., barcode readers)
	Laboratory Instrumentation*
	Laboratory Information Management System (LIMS) Applications**

*Laboratory instruments include complex computer systems to collect and analyze data and transmit this data to the LIMS.

**The LIMS is among the most important technologies in the laboratory. Optimal LIMS maintenance and management require specialized knowledge of laboratory operations.

4. A USER'S GUIDE TO SUCCESSFUL IT SERVICES NEGOTIATIONS (CONTINUED)

4.1.1 IT Technologies Necessary for Successful Laboratory Operations (continued)

Because of its centrality to laboratory operations, the LIMS warrants special attention in any service negotiations. Several key points should be communicated:

- The LIMS provides the infrastructure for efficiently logging and accessing clinical and environmental test data and electronically reporting findings to data stakeholders.

- LIMS are typically directly connected to analytical instruments and become an integral part of the analytical process.

- Because LIMs are shared resources on a national/global level, they must comply with federal data-sharing requirements.

- LIMS often incorporate other business processes essential to internal functioning, such as billing, inventories and quality control processes.

- LIMS design is the result of a collaborative process involving multiple entities. The basic architecture is based on hundreds of requirements spanning 16 business processes applicable to a wide range of public health laboratories.[12] Some, but not all, commercial, off-the-shelf LIMS meet these general requirements and are ready for immediate implementation. These products eliminate the need for each laboratory to create a system independently, from the ground up. Nonetheless, additional configuration and customization is nearly always needed to meet unique laboratory needs.

- Long-term, successful LIMS operation requires extensive planning and appropriate budgeting for system design, acquisition, installation and ongoing maintenance, customization and upgrades.

Figure 2 illustrates the many data handling services LIMS perform in the laboratory.

> "The main barriers to LIMS sustainability are piecemeal funding streams and lack of in-house expertise in IT and informatics."
>
> *Moving Toward Interoperability: Laboratory Information Management Systems and Meaningful Use of Laboratory Data,* APHL Collaborative White Paper, December 2009
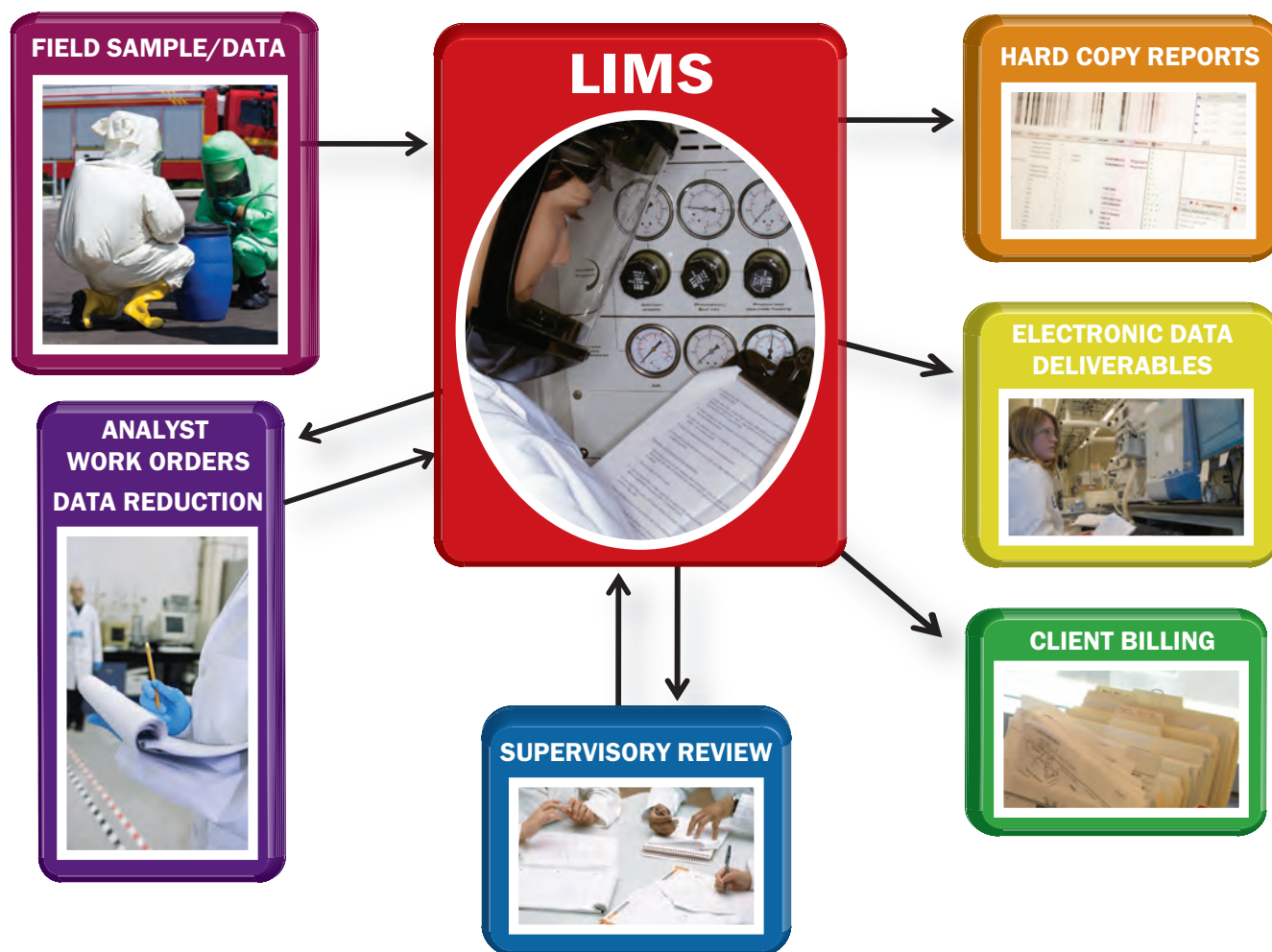
In September 2009, the Virginia Division of Consolidated Laboratory Services implemented a comprehensive LIMS that was recognized by NASCIO for "enhancing intergovernmental collaboration, planning, performance, transparency, fiscal accountability, cross-jurisdictional services and intergovernmental transaction processing." The system's use of common data standards and integration of laboratory instrumentation and audit and management tools reduces the need for manual data entry and allows a greater focus on testing. Automated quality control and validation protocols ensure compliance with good laboratory practices and federal regulations. Barcode technology tracks samples. Maintenance and other technical support needs are simplified via a common architecture. And data resides in a database configured for high availability in a secure server environment.

---

(12) 2003 Requirements Document Publication -16 PHLs, Association of Public Health Laboratories, Public Health Informatics Institute, Centers for Disease Control and Prevention, Public Health Information Network,
http://www.aphl.org/aphlprograms/informatics/Pages/requirementslims.aspx.
Last accessed April 14, 2011.

FIGURE 2. LIMS DATA HANDLING SERVICES

4.1.2 IT Governance and Technical Support

IT governance and support activities enable laboratory staff to make effective use of commercial hardware and software, while also allowing the organization to manage these assets over time as needs evolve. As shown in Table 2 (page 13), these activities include everything from allocating bandwidth for data transmission to assuring the availability of a 'help desk' to respond to users' service requests.

TABLE 2. IT GOVERNANCE AND TECHNICAL SUPPORT ACTIVITIES	
✓	
	Integrate analytical instrumentation into data collection and reporting systems.
	Store and retrieve large amounts of analytical data, with fully redundant systems to ensure zero data loss and continuity of operations.
	Achieve interoperability with the data systems of major partners—including relevant state and federal agencies—so data can be transmitted in near real-time.
	Provide the necessary bandwidth for data communication.
	Meet the complex reporting and data security requirements dictated by federal laws and regulations (e.g., Clinical Laboratory Improvement Amendments, Health Insurance Portability and Accountability Act, etc.).
	Maintain electronic security for infectious and toxic agents, with access restricted to personnel with appropriate federal security clearances.
	Provide for rapid, scalable 24/7 emergency IT support.
	Manage fiscal and business IT needs.
	Provide operational services, such as system back-ups.
	Maintain an IT 'help desk' capable of responding to potentially dozens or hundreds of service requests daily.
	Provide staff training on topics ranging from desktop software to regulatory IT requirements.
	Develop/customize software as needed.
	Support a management infrastructure with policies, practices, accountability and commitment.
	Provide for other miscellaneous needs: modernization of legacy systems, IT security enhancement, records management, etc.

4. A USER'S GUIDE TO SUCCESSFUL IT SERVICES NEGOTIATIONS (CONTINUED)

4.2 The MOU and SLA

Memoranda of understanding (MOU) and service level agreements (SLAs) are the two major tools recommended for IT services negotiations and ongoing management. IT and laboratory leaders can use these tools to communicate and document the costs, risks and metrics of laboratory IT services. The documents must convey the importance and functions of laboratory services, but be written in the language of the IT professional.

In the case of consolidation, laboratory leaders may not have the option of IT negotiations culminating in a signed MOU and SLA. Nevertheless, it will be beneficial to document the IT activities that are necessary for successful laboratory operations. Moreover, a written account of laboratory IT needs may serve as a door opener to at least informal IT discussions.

> "IT costs consume a large part of our organizational revenues. Laboratory management must ensure that these resources are used effectively and efficiently. An effective partnership with a shared services provider can play an important role in good public health laboratory informatics operational strategy."
>
> **Garrett Peterson**
> **Division of Public Health Informatics**
> **Wisconsin State Laboratory of Hygiene**

No matter what shared services model is used, it is advantageous to negotiate a MOU and SLA with the jurisdiction's IT managers. These documents must be written in terms familiar to the CIO, with clear business case models. The MOU—discussed further below—is the more general of the two and defines the role of each of the governmental partners. The SLA—which is not addressed in depth in this document—is more granular and presents the details of IT delivery, including a funding model for laboratory technology initiatives and infrastructure. The SLA also generally includes metrics to define acceptable outcomes, as well as the risks associated with failure to comply with the terms of the agreement. A critical component of both the MOU and SLA is the approval page, which must be signed by high-ranking organization representatives.

Once the MOU and SLA are in place, continued dialogue and negotiation are essential to provide feedback on the documents' implementation, maintain a close working relationship with IT managers and offer guidance for the future.

4.2.1 Getting Ready to Negotiate

The following activities should take place before any IT negotiations begin.

Identify IT Leaders and Their Priorities
Invest the time to understand the drivers behind the organization's IT efforts so you know whom to engage and how best to approach the conversation.

Plan to Explain the Work of the Laboratory
Successful IT negotiation begins with the recognition that IT leaders do not speak the language of the laboratory and likely have scant familiarity with laboratory operations and necessary LIMS functionality. Thus, laboratory leaders must be prepared to explain core laboratory activities.[13]

....
(13) A useful reference on PHL activities is *Core Functions and Capabilities of State Public Health Laboratories: A Report of the Association of Public Health Laboratories,* MMWR 2002;51 (No. RR-14):1-8, available at www.cdc.gov/mmwr/preview/mmwrhtml/rr5114a1.htm.

4. A USER'S GUIDE TO SUCCESSFUL IT SERVICES NEGOTIATIONS (CONTINUED)

Document the Laboratory Business Case

Prepare a document—using terms that are clear to both laboratory and IT leaders—laying out the laboratory's operational and business framework:

- The laboratory's vision statement;
- A description of core laboratory business activities;
- Top business priorities for the year;
- Business performance metrics;
- IT priorities aligned with business priorities;
- The names of laboratory leaders who will sign off on the MOU and SLA(s) and serve as liaisons with the jurisdiction's IT leadership.

Identify Costs

The MOU and SLA need to identify all IT activities necessary to support a laboratory. As mentioned above, these generally fall into three categories: technologies, governance functions and technical support activities. *Identify the current, true operational and capital expenses associated with each item or activity using the checklists comprising Tables 1 and 2.* In the course of this exercise, it is especially helpful to describe each item or activity in the context of the laboratory business case. This comprehensive catalog will be the basis for negotiating the cost of shared IT services and, ultimately, the metrics used to gauge adequate service delivery. (Metrics, in turn, will include measures such as hours of downtime, frequency of back-ups, etc.)

Segregate Services That Must Be Managed Locally

Catalog all of the IT services your laboratory uses and determine which are unique needs/requirements that should/must be managed locally and which can be provided at an enterprise level. For example, LIMS support is likely to include activities that are best managed locally, while e-mail support is likely an activity that can be effectively managed off-site.

Identify Risks

Every IT environment has inherent risks. Examples include:

- Impacts of service disruptions on laboratory operations and customers (e.g., delays in delivery of newborn screening results).
- Potential financial, legal or public relations impacts of the inadvertent release of private medical information or other data.
- Consequences associated with loss of archived data or other assets.
- Legal consequences associated with failure to comply with federal laws and regulations.
- Impact on continuity of operations and incident command structure associated with non-redundant or inadequately 'scalable' systems or support functions (e.g., inability to provide adequate support during periods when surge capacity is needed).
- Budgetary risks of catastrophic failure of expensive infrastructure components.
- Organizational risks of insufficient staffing redundancy for IT operations.
- Opportunity costs associated with lack of agility to take advantage of new ideas, new technologies, funding opportunities or other circumstances due to fragile or non-flexible policies, systems or IT infrastructure.

Plan for Handoffs

Identify the resources or activities necessary for IT transitions. For instance, laboratory staff must understand their roles and responsibilities associated with new system roll-outs (e.g., system testing). Similarly, there must be a clear channel of communication to enable IT staff to coordinate periods of downtime to avoid disruptions of service and to quickly scale-up support during operational surges.

Participate in IT Governance

Of course, if there is no participation in IT governance, laboratory leaders will have little opportunity for direct negotiations. However, going forward, leaders must insist upon a 'seat at the table' so there is adequate laboratory representation on any standing IT governance body.
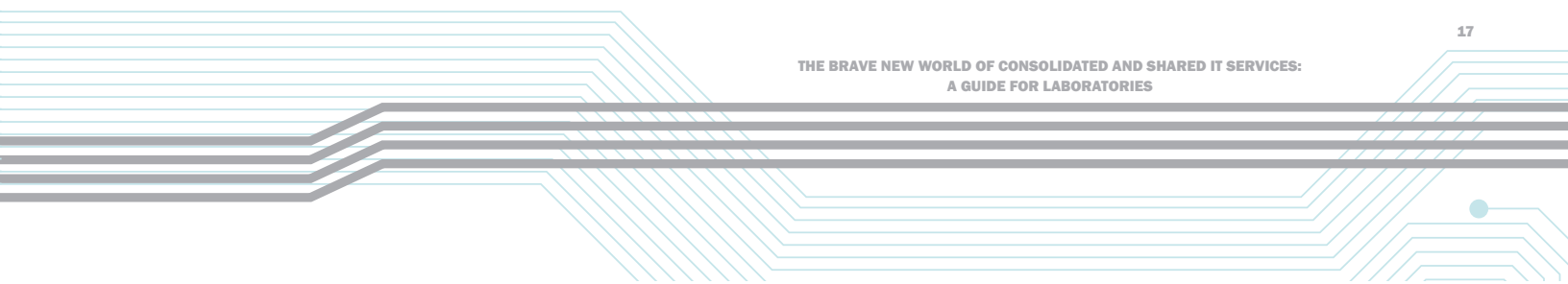
4.2.2 Potential MOU Provisions

Although each laboratory operates within a unique political and business environment, there are some vital, common needs that every laboratory leader in a shared IT services arrangement should consider incorporating into an MOU.

1. **Prioritizing the LIMS as a critical adjunct to laboratory instruments and a core component of the laboratory infrastructure.** The LIMS is the primary node for collecting laboratory data from instruments and creating electronic messages or other automated reports to share with partners. As such, there may be distinct advantages to setting up the LIMS as a server on the local laboratory network so that laboratory users have an isolated, fully functional application environment, with few, if any,components shared with non-laboratory users. In any case, performance considerations may make it difficult (and undesir-able) to host certain LIMS applications—e.g., instrument and equipment interfacing for real-time data transfer—at a central location.

2. **Prioritizing the need for dedicated application level LIMS support.** Even with the use of a collaboratively developed LIMS, there is a need for dedicated IT staff to support laboratory data management. Having support staff at the programmatic level facilitates familiarity with the laboratory's business needs, custom applications and instrumentation interfacing.

Dedicated LIMS personnel may also be key to continuity of operations plans and surge capacity for all-hazard events.

3. **Assuring 24/7 on-site support.** Even with a 24/7 maintenance agreement with a LIMS vendor, there is a need for onsite staff who understand the instrument interfacing; data querying/data release issues; regulatory requirements; application changes; and novel issues that arise during an outbreak or other event requiring rapid deployment of new code, rapid review of data reports and data quality management while messaging between partners. It is unrealistic to expect shared, central IT staff to acquire and remain current with this specialized knowledge and to be available as needed (See #7 below).

4. **Assuring authority to manage vendors.** The laboratory should not cede its authority to monitor vendor performance and ensure that the terms of agreements are being enforced or updated, as necessary.

5. **Addressing security clearances and protection of personal identifiers in laboratory data**. Application support staff must have appropriate security clearance as required under the CDC's select agent rule and the Clinical Laboratory Improvement Amendments.

6. **Defining partnerships with high visibility agencies within your state and/or local government that have a governance role in IT affairs.** Each jurisdiction has its own approach to integrating laboratory services for health, emergency response, regulatory and law enforcement activities. It may be necessary to educate partners about laboratory requirements and priorities.

7. **Prioritizing IT support for emergency response activities.** Computer applications that support emergency response activities—and particularly those related to biological and chemical threat response—require 24/7 support to ensure the applications are up and running during crises. Laboratory IT support staff, working alongside scientific staff during such events, prioritize their activities to meet critical needs.

8. **Assuring oversight and project management at the laboratory level.** Analytical oversight and management at the laboratory level is needed to periodically interpret and implement any application changes to ensure consistency with business needs and regulatory requirements. Such oversight leads to better service, improves business visibility, fosters effective decision-making and helps to maintain organizational knowledge.

4. A USER'S GUIDE TO SUCCESSFUL IT SERVICES NEGOTIATIONS (CONTINUED)

There are numerous references for MOUs and SLAs. Figure 3 depicts a sample SLA/MOU table of contents used by the US Department of Health and Human Services.

FIGURE 3. SAMPLE SLA/MOU TEMPLATE

TABLE OF CONTENTS

1   INTRODUCTION
   1.1   Purpose of Service Level Agreement/Memorandum of Understanding
   1.2   Scope
   1.3   Background
   1.4   Audience
   1.5   Assumptions
   1.6   Roles and Responsibilities
   1.7   Contacts

2   SERVICE DETAILS
   2.1   Requirements
   2.2   Service Level Expectations
   2.3   Escalation Actions
   2.4   Service Provider / Service Recipient
   2.5   Service Hours for Problem Resolution
   2.6   Performance Guarantee
   2.7   Agreement Change Process

3   AGREEMENT TABLE

   APPENDIX A: SLA/MOA UNDERSTANDING APPROVAL

   APPENDIX B: REFERENCES

   APPENDIX C: KEY TERMS

Source: US Department of Health and Human Services. Available online at http://www.hhs.gov/ocio/
eplc/EPLC%20Archive%20Documents/50-SLA%20and%20MOU/eplc_sla_mou_template.doc.
Last accessed May 2011.

5. CONCLUSION

Acquiring the IT assets and skills necessary to keep a state-of-the-art laboratory operational is costly, and may be more expensive than CIOs and laboratory leaders may realize. Engaging with partners to consolidate some or all IT services could enable governmental laboratories to access better and more effective information technology than they can afford or support alone. In any case, in jurisdictions where IT consolidation or shared services is mandated from above, laboratory leaders must be prepared to advocate on their organization's behalf.

The negotiation process outlined in this paper includes:

- Working with internal IT leaders to lay out the laboratory business case and, within the business case, necessary IT services, such as those included on the checklists comprising Tables 1 and 2.

- Going into negotiations with state IT leaders knowing IT services (including those that are best managed in-house), costs, risks and performance metrics.

- Documenting IT services agreements in a formal MOU and SLA with appropriate laboratory signatories.
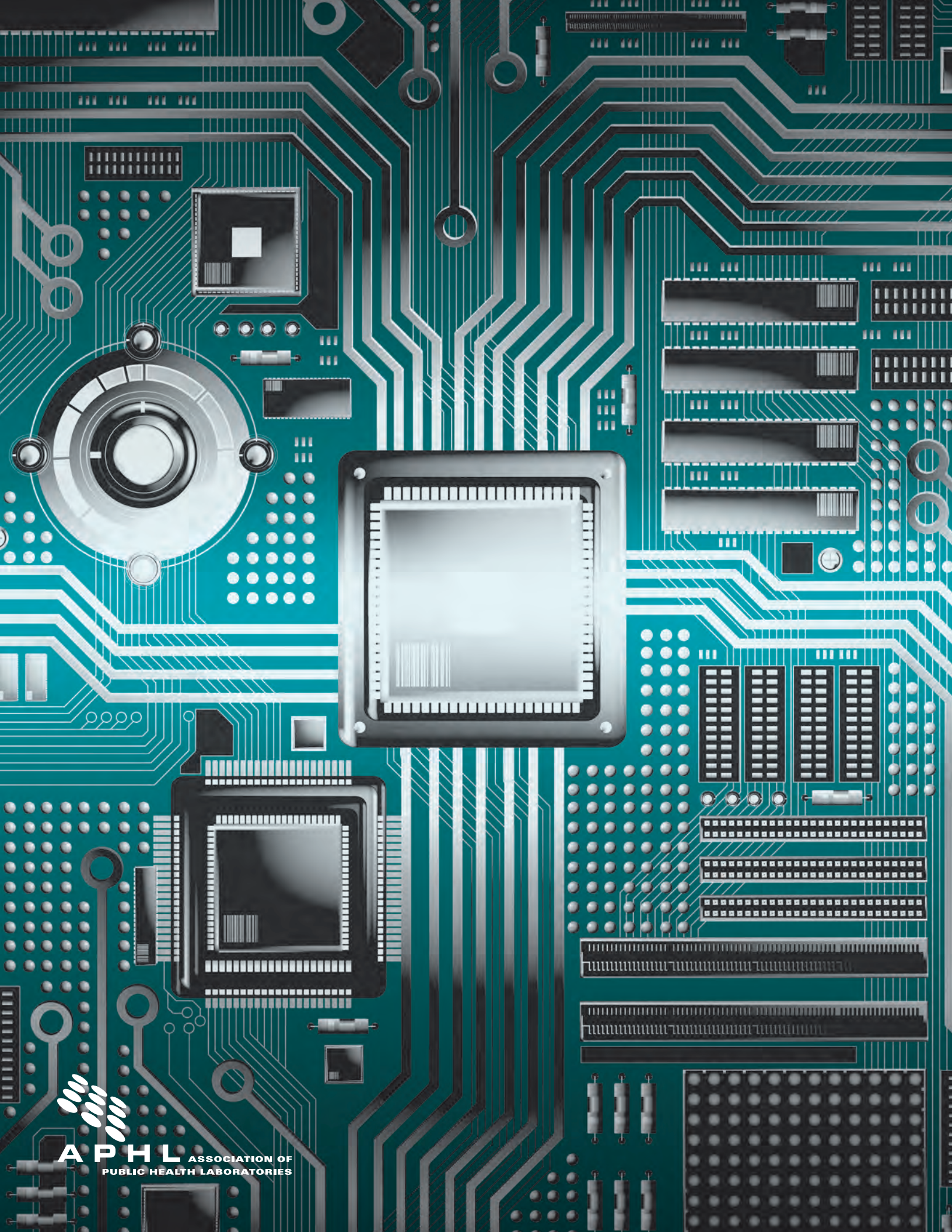
With a thoughtful approach to consolidated and shared IT service negotiations, along with input from IT and laboratory stakeholders, laboratory processes and information exchange can be improved—but to what degree, given the rapid advancements of IT solutions and the changing landscape of laboratory informatics, remains to be seen.

Association of Public Health Laboratories
8515 Georgia Avenue, Suite 700
Silver Spring, MD 20910

APHL **ASSOCIATION OF PUBLIC HEALTH LABORATORIES**