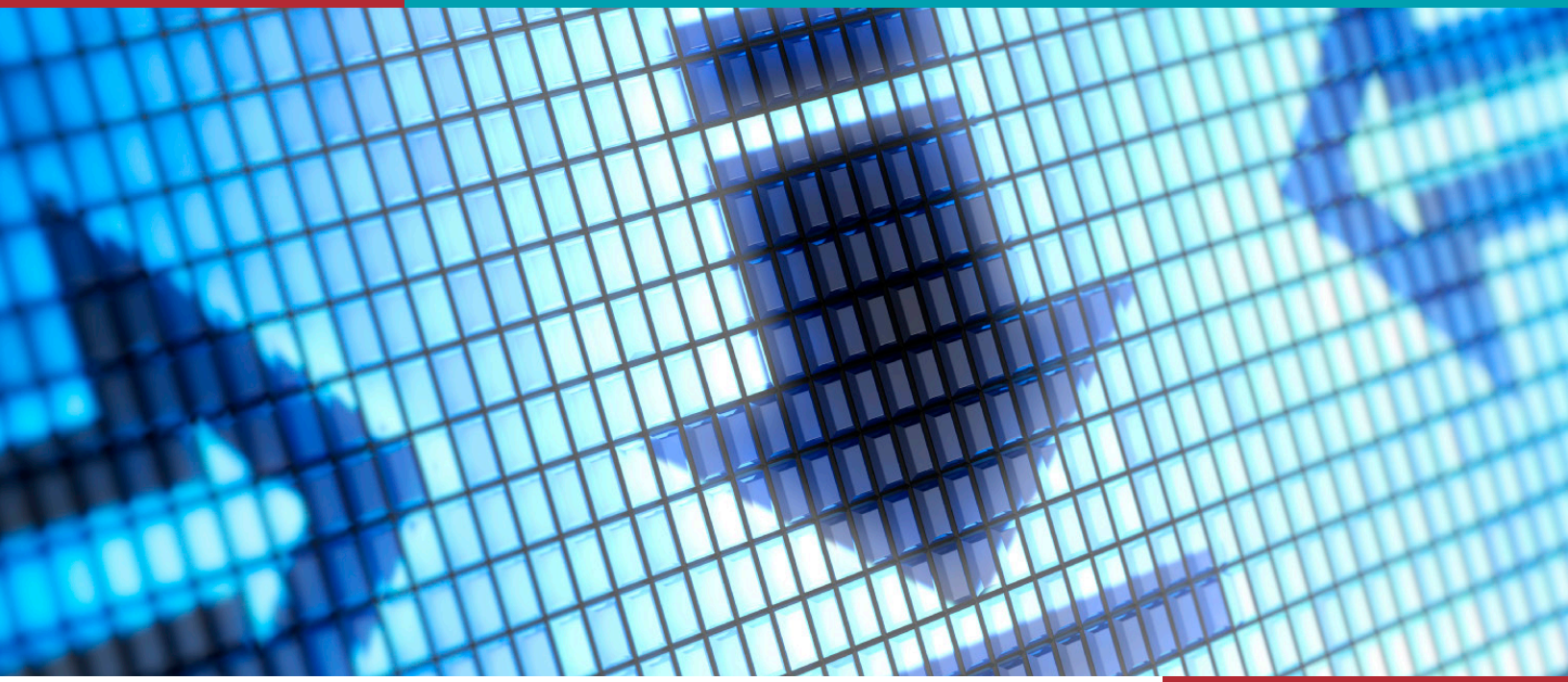
The Brave New World of Laboratory Informatics II:

Navigating in the Digital Age



OCTOBER 2015

APHL ASSOCIATION OF PUBLIC HEALTH LABORATORIES™

This publication was 100% funded with federal funds from a federal program of $ 3,093,643. This publication was supported by Cooperative Agreement # U60HM000803 funded by the Centers for Disease Control and Prevention. 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.
National Center for Immunization and Respiratory Diseases (IP)
Office of Surveillance, Epidemiology and Laboratory Services (OSELS)
National Center for HIV, Viral Hepatitis, STDs and TB Prevention (PS)
National Center for Zoonotic, Vector-borne, and Enteric Diseases (CK)
National Center for Environmental Health (NCEH)
Coordinating Office for Terrorism Preparedness and Emergency Response (CTPER)

Table of Contents

I. Introduction and Background 2

II. PHLs Need a Reliable, Flexible IT Infrastructure 3

Building Information Technology to Support Laboratories 5

III. Laboratory Informatics Solutions 6

Enterprise Informatics Solutions 7

Case Study 1: Managing Newborn Screening Records in Kentucky 10

Case Study 2: Sharing Environmental Test Data in New Jersey and Nationally 11

IV. Legal and Procedural Considerations 12

Memorandum of Understanding (MOU) — A High-level, General Agreement 12

Service Level Agreement (SLA) — A Contract for Specific Services 13

V. Conclusion 16

References 18

Acknowledgements 19

I. Introduction and Background

A modern public health laboratory (PHL) is a complex environment and the business of PHL practice grows more complex daily. Nonetheless, the laboratory's core commodity remains unchanged: information.

Today, laboratory stakeholders expect this information to be more comprehensive and to flow faster and more securely than ever before, both to satisfy the needs of external clients and to improve internal operations by managing the laboratory's inherent complexity.

Laboratory informatics — the specialized application of information technology to optimize laboratory information management — is essential to enable PHLs to deliver information in timely fashion and in standardized electronic formats. In addition, although electronic information management may not always be cheaper than manual alternatives, it reduces errors, reduces dependency on one-off processes that are difficult to maintain long-term and promotes uniformity and agility in the laboratory. In short, laboratory information technology (IT) services are now a mission-critical component of PHL operations.

The brave new world of laboratory informatics represents a clear break from the past, when laboratories had complete control over their information management activities. Instead, a new information management model has been widely adopted by government jurisdictions: the shared services model, in which PHLs maintain their decentralized control over several core activities — such as laboratory information management system (LIMS) selection, report formats, etc. — but have lost decision-making authority over the IT infrastructure supporting these activities.

As discussed in the 2011 APHL report, *The Brave New World of Consolidated and Shared IT Services: A Guide for Laboratories*,[1] **shared services** is the centralization of information technology and business functions that are carried out by multiple government entities (e.g., billing) to gain economies of scale. The centralized resources and services can then be leveraged across the entire government agency or enterprise, resulting in lower, overall IT costs at the enterprise level and access to more sophisticated IT services, technology and talent than individual public health programs could afford on their own.

Shared services models may or may not employ another relatively recent IT phenomenon, **cloud computing** — the delivery of hosted informatics services via the Internet (i.e., the "cloud").

Whatever model of IT service delivery your jurisdiction has adopted — or is moving toward — it is important to be a proactive participant and leader in the enterprise setting. Familiarity with the brave new world of laboratory informatics will help you advocate for your institution in the forums available to you and, ultimately, to influence agency decisions impacting the laboratory. But remember, in order to raise the enterprise's awareness of laboratory needs, you must first raise your awareness of the enterprise and have at least a general understanding of possible laboratory informatics solutions. That is the focus of this document.

---

* The term *shared services* is often used interchangeably with *IT consolidation*, and even the National Association of State Chief Information Officers acknowledges that they "seem to be two flavors of similar endeavors." Nonetheless, NASCIO defines them differently. *Shared services* are specific services centralized to gain economies of scale; participation may be voluntary or based on organizational consensus. The term consolidated services implies organizing delivery of all IT services "into a single operation, typically mandated by executive order or statute." Thus, according to APHL's 2011 report *The Brave New World of Consolidated and Shared IT Services: A Guide for Laboratories*, "shared services may be one step on the road to consolidation or consolidation may be viewed as a case of all-inclusive shared services."

II. PHLs Need a Reliable, Flexible IT Infrastructure

In 2003, APHL and the Public Health Informatics Institute identified 16 business processes relevant to public health laboratory operations and outlined LIMS requirements specifications for each.[2] These processes include everything from clinical and environmental test processing to lab certifications/licensing to disaster recovery. Since then, it is safe to say that many, if not most, of these processes have grown more complex, along with their associated information management needs.

Moreover, while the LIMS is a critical asset, laboratory leaders must also take account of the larger IT infrastructure, which includes:

- **Governance functions**, such as budgeting for IT products and services, contract oversight, development of IT policies and other management activities.
- **Technical support**, including software customization, staff training, trouble-shooting and other activities to implement commercial technologies and assist end-users.

One forward-looking — and inescapable — example of increasing laboratory complexity is bioinformatics. Since completion of the federal Human Genome Project in 2003, genetic sequencing technology has become faster, more affordable and more compact, now available in benchtop instruments such as Life Technologies Ion Torrent™ and Illumina's MiSeq. A recent advance is the development of direct read technologies, negating the need for intensive pre-amplification of pathogenic nucleic acids. The improved technology, in turn, has sparked an explosion of interest in genomics assays.

The problem for the laboratory is that these next-generation genomic assays generate magnitudes more data than ever before — terabytes and petabytes of data instead of megabytes and gigabytes. Rather than providing eight- to ten-fold coverage of target genomes, newer instruments provide deep 20,000-fold coverage, producing smaller and more noisy, error-prone reads of RNA or DNA fragments, which then have to be reassembled to recreate the genome. At the same time, laboratories may be running batches of 94 samples at once in a high-throughput assay.

Processing such huge amounts of information requires (1) higher orders of computing ability, perhaps involving clusters of networked servers; (2) expertise to implement intricate software to translate complex mathematical models into functional algorithms; and (3) vast amounts of secure, high-speed storage.

Data storage alone may be a significant problem, depending on the information a laboratory needs to maintain long-term for regulatory, clinical and public health purposes. In addition to producing test results that are used and then discarded, governmental laboratories are increasingly producing information that must be available for reexamination in the context of new problems and new information. Since sequencing one *Salmonella* genome can produce a terabyte of data, it is easy to see that reference databases can get very big, very fast. Then, comparing test results with stored datasets can pose a fairly large informatics problem in and of itself, requiring access to high-performance computing.

Looking ahead, public health, agricultural and environmental testing laboratories can expect to continue their traditional role as an analytics engine for public health, while at the same time becoming a greater part of the solutions engine.

It is not a stretch to envision public health laboratories carrying out their diagnostic and surveillance functions in new ways in the future:

- Tapping multiple reference libraries to detect all known genetic anomalies in a newborn screening specimen.
- Using high-performance computing to determine why a specific genetic change impacting one protein confers antibiotic resistance to a newly detected *M. tuberculosis* serotype.
- Examining multidimensional data to better understand phenotypic traits influenced by multiple genes and epigenetic factors.
- Examining influenza genetic markers to study viral rates of change to better predict the optimal composition of the next season's flu vaccine.

This evolving role will require more mathematics, more computing and more algorithmic programming.

In short, public health and other governmental laboratories need a reliable, flexible IT infrastructure that can scale to adapt to increased complexity or volume within the laboratory. Moreover, this infrastructure must be reasonably secure to guard against accidental or intentional misuse.

"There are a number of considerations to finding the right IT solution for the problem you're trying to fix. As we move into genomics, a number of issues typically come up, whether you have an on-site or cloud-based server for your instrument. In Idaho, we've gone with an on-site server.

From my perspective, the large volume of data involved with genomic testing is a potential problem. But this could be resolved by determining which files you need to move. If you do a lot of analysis in-house and you feel comfortable with the quality of the final product, you end up with a relatively small text file, and that's all you need to move around.

For many public health laboratory applications, we're not going to be doing the types of analyses you see in the academic world. I think we need to agree on quality parameters — for depth of coverage at each locus and breadth of coverage across the genome — for the information we need to share over a secure messaging infrastructure. We need to have national standards, and, inevitably, we're going to have to sacrifice analytical complexity to get to something that's practical and can be standardized in multi-site evaluations.

If you have the ability to demonstrate how you got to the final product, how much data do you need to store for reanalysis? At a certain point, it's going to be easier to take the isolate out of the freezer and reanalyze it, rather than finding the data."

Christopher L. Ball, PhD, HCLD (ABB)
Chief, Idaho Bureau of Laboratories

Building Information Technology to Support Laboratories

As a laboratory's need for information technology continues to grow, there is a balance that must be struck between what is built in-house and what is outsourced. This decision has ramifications on the laboratories' ability to meet its future needs, provide customer satisfaction and reduce operating cost. Furthermore, there are strategic decisions to be made regarding whether external services are to be provided through state resources or through other means. Choosing the right resource for services — internal or external — must be part of an overall laboratory strategy that defines and supports the desired outcomes.

In an article published by *McKinsey & Company,* "To centralize or not to centralize," the authors pose three questions that can help senior managers make better choices about what service to centralize and what to decentralize: 1) Is centralization mandated? 2) Can it add 10 percent to a corporation's value? And 3) Can it be implemented without negative side effects?[3]

> *A proposal to centralize only needs a "yes" to one of these three questions. Yet they provide a high hurdle and can help managers avoid too much centralization. Moreover, they stimulate open and rational debate in this highly politicized area. By giving those in favor of centralization and those opposed to it a level playing field for building a case, these questions help companies strike the right balance between centralization and decentralization today and to evolve their organizations successfully as conditions change over time.*

Beside costs, there are other factors that affect centralization and decentralization, such as access to skilled workforce. While labs could once reassign bench scientists to learn how to handle IT operations, they now need access to highly trained IT professionals, such as bioinformaticians, security analysts, database administrators, a virtualized infrastructure manager, network specialists, data messaging/vocabulary specialist and software developers with various expertise. Although laboratories may not need the full time services of each of these specialists, they are unlikely to find one person qualified in multiple areas. For example, a security analyst will probably not have messaging or vocabulary expertise and a bioinformatician will probably not have database administration skills.

Similar to laboratory functions such as sample receiving, result reporting, or billing, IT services can be grouped and evaluated for factors like cost, availability of staff, strategic direction, or potential growth. Some of these services are becoming available as a commoditized service. For example, email and calendaring has become such a universal service that most organizations have centralized and many now use cloud-based versions of these products. On the other hand, services such as LIMS development, building web portals for client access or instrument interfacing should likely continue to be performed by dedicated laboratory IT staff because of the specialized knowledge required and the fact that these functions often provide mission critical differentiation of the laboratory services in the eyes of its customers.

The IT technology in a laboratory must be able to grow and adapt to the changes that the business dictates, and that is capability that commodity service providers will never be able to address adequately.

III. Laboratory Informatics Solutions

The informatics solutions available to a laboratory depend, in large part, on the laboratory's current informatics capabilities or so-called *IT maturity level*. In fact, a basic understanding of a laboratory's IT strengths and limitations is the cornerstone for long-term informatics planning in a comprehensive, systems-oriented fashion.

To facilitate the planning process, APHL and CDC developed the *Informatics Self-Assessment Tool* for Public Health Laboratories.[4] The tool — available at http://www.aphl.org/aphlprograms/informatics/collaborations/Pages/LEI-Informatics.aspx — was designed to help laboratory leaders identify gaps in informatics capabilities, identify and prioritize actions to fill those gaps, facilitate communications with agency IT managers and other government leaders and to monitor informatics capabilities on an ongoing basis.

Released in 2013, the self-assessment tool is based loosely on the Carnegie Mellon Capability Maturity Model℠ (CMM), which was developed in 1993 with funding from the US Department of Defense to assess the ability of government contractors to carry out software development projects. The model — now widely used to assess IT service management, in general — ranks relevant processes on a five-tier scale progressing from *initial* (i.e., chaotic or ad hoc) to *repeatable* (i.e., with project tracking and oversight) to *defined* (i.e., with documented standards) to *managed* (i.e., using quantitative process metrics) to *optimizing* via change management and continuous quality improvement.[5]

The APHL tool is organized around public health laboratories' 16 business processes, which it translates into the 19 capability areas listed in Table 1. Each capability applicable to the laboratory is ranked on a three-tier scale:

- Maturity Level 1: No/very little current ability to execute the functions described
- Maturity Level 2: Minimal required technology and process in place to execute the functions described
- Maturity Level 3: Technology and process in place/extended to execute the functions described beyond the local business domain

A maturity Level 3 laboratory, for example, is able to receive an electronic test request message from a submitter for all tests; able to automatically bill customers for non-test services provided; able to use informatics technologies to facilitate quality management system analytics; and able to preserve instrument data and reprocess them when the LIMS is restored following a network or system failure.

Eventually, APHL hopes to publish summary statistics describing the overall informatics maturity level of the US public health laboratory system, along with a list of any areas needing further development. (In general, public health laboratories tend to be at higher maturity levels than state agricultural and environmental testing laboratories.)

Once a laboratory has prioritized its informatics needs, it may be able to develop discrete capabilities in-house, ideally employing a limited set of technologies for multiple processes and data-exchange partners. Likely, however, the laboratory is subject to enterprise informatics policies and will also be able to (or be required to) take advantage of enterprise solutions.

Table 1. 19 Laboratory Informatics Capability Areas (CAs)*

CA #1	Laboratory Test Request and Sample Receiving
CA #2	Test Preparation, LIMS Processing, Test Results Recording and Verification
CA #3	Report Preparation and Distribution
CA #4	Laboratory Test Scheduling
CA #5	Prescheduled Testing
CA #6	Specimen and Sample Tracking/Chain of Custody
CA #7	Media, Reagents, Controls: Manufacturing and Inventory
CA #8	Interoperability and Data Exchange
CA #9	Statistical Analysis and Surveillance
CA #10	Billing for Laboratory Services
CA #11	Contract and Grant Management
CA #12	Training, Education and Resource Management
CA #13	Laboratory Certifications/Licensing
CA #14	Customer Relationship Management
CA #15	Quality Control and Quality Assurance Management
CA #16	Laboratory Safety and Accident Investigation
CA #17	Laboratory Mutual Assistance/Disaster Recovery
CA #18	Core IT Services: Hardware, Software and Services
CA #19	Policies and Procedures, including Budgeting and Funding

**Source: APHL and CDC. (2013). Laboratory Efficiencies Initiative: Informatics Self-assessment Tool for Public Health Laboratories. Silver Spring, MD: APHL. Retrieved from: http://www.aphl.org/MRC/Documents/LEI_2013Jun_Informatics-Self-Assessment-Tool-for-PHLs.pdf*

Enterprise Informatics Solutions

Agency-wide or *enterprise* informatics policies set baseline IT requirements and standards. Such policies are based on accepted national and industry standards, are product independent and allow for expansion. As detailed in Table 2, successful, centralized IT governance boosts efficiency, effectiveness and information security. In fact, shared or consolidated IT services are attractive to government and large corporate entities precisely because they reduce risks and save money, at least at the enterprise level.

The state of Montana, for example, uses 2,878 virtual servers or VMs (virtual machines), with each physical host providing up to 30 VMs.[6] If Montana were fully centralized, the State Information Technology Services Division (SITSD) calculates that savings would be on the order of $2.5 million/year, compared with a decentralized infrastructure. Annual savings would include:[7]

- $1.4 million for servers ($480,000 with centralization vs. $1.9 million without)
- $942,000 for maintenance and support ($198,000 vs. $1.14 million)
- $178,500 in lower energy consumption

Currently, Montana agencies pay about $265/year per terabyte data storage, while the SITSD pays $46/year per terabyte for its centralized data storage.[8] The high agency costs are partly due to the substantial amount of unused storage space on agency storage devices (about half). In addition, because the state procures computer hardware and services in greater volumes than any individual agency, it is able to negotiate lower prices and more favorable terms from IT vendors.

Table 2. Centralized IT Governance: More Efficient, Effective, Secure

Efficient

- Reduced and optimized IT expenditure per unit
- Elimination of duplicate IT systems
- Improved purchasing power via combined procurement agreements
- Cost savings from hardware and software standardization, e.g. management reports

Effective

- Industry-standard delivery of IT services and, thus, enhanced service reliability
- Improved ability to align IT resources with high-level government priorities
- Improved data-sharing capabilities

Secure

- Improved data protection
- Fewer IT systems hosted at insecure locations
- Firewalls
- Swifter detection of attempted security breaches, alerting and response
- Redundant power and cooling systems
- Separate data backup site
- Controlled access and dual internet access (for redundancy)
- Fire suppression

Enterprise services offer other benefits, as well:

- A variety of best-in-class products and services, including shared or dedicated IT platforms to support a variety of system types
- Standardized implementation and common best practices
- Customization, when needed
- Timely hardware and software updates
- Improved application performance due to system monitoring
- Strengthened relationships with business partners and other governmental units
- Improved employee morale due to more clearly defined job roles and improved work flow

Common, core enterprise services include an IT help desk with 24/7 emergency support; consulting and software customization services; server, data storage and software application hosting; and secure maintenance of mission critical infrastructure.

Among the prime public health candidates for centralization are application hosting (e.g., accounting software), data mining services, services to assure compliance with federal IT standards, and interoperability and brokerage services, such as HL7 messaging and message format conversion. As always, the business case must drive the technology and the organization of IT services.

Because electronic messaging, in particular, is such a ubiquitous challenge, APHL has developed its own shared services solution, the APHL Informatics Messaging Services (AIMS) platform — a secure, cloud-based environment that simplifies the validation, translation, transformation and routing of electronic public health data. The AIMS platform is FedRAMP (Federal Risk and Authorization Management Program), FISMA (Federal Information Security Management Act) Moderate and HIPAA compliant — a status that may be difficult to attain with an on-premise datacenter. In spring 2015, the platform had more than 50 messaging partners routing more than 10,000 messages/month, on average, through the system.

Among other things, the AIMS platform has been used to transport messages related to possible bioterrorism threats and to maintain pandemic influenza surge capacity for electronic laboratory test orders and results reporting (ETOR).

Following are three case studies, from Kentucky, New Jersey and CDC that show how shared services are being used to craft informatics solutions.

From left: Keith Higginbotham, Neelima Vundela, Dr. Sharon Massingale, Ron Howard

"The Alabama Department of Public Health's Bureau of Clinical Laboratories has an exceptional relationship with our department's Bureau of Information Technology. The bureau provides physical and electronic security services, a shared messaging environment for data exchange with internal and external clients, technical resources to handle our computing hardware and technical expertise for joint LIMS administration. It would be difficult for the laboratory to replicate these services independently."

Sharon P. Massingale, PhD HCLD/CC(ABB)
Director, ADPH Bureau of Clinical Laboratories

Case Study 1: Managing Newborn Screening Records in Kentucky

Background

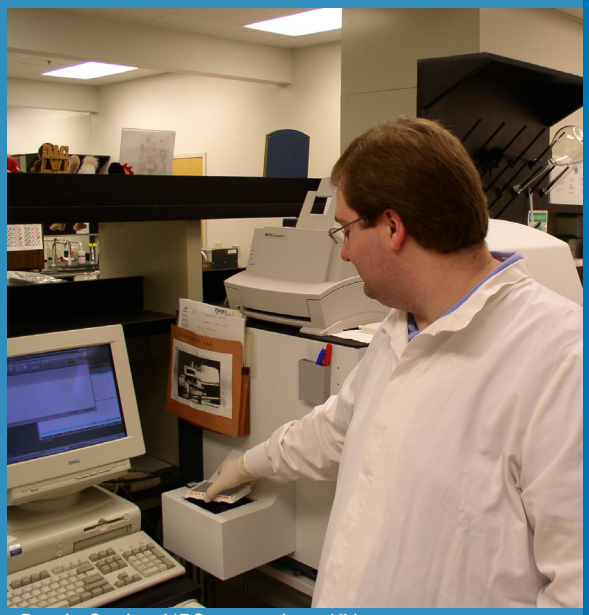
The Kentucky Division of Laboratory Service tests about 60,000 newborn screening (NBS) specimens each year for 50 different disorders, generating roughly 3 million test results annually. Historically, this data has been reported both to providers and to the Kentucky Health Information Exchange (KY HIE), which also provides access to patient data from the state immunization registry, cancer registry and other sources.

Problem

Each year, there are hundreds of Kentucky newborn screening specimens sent to the laboratory for as-yet-unnamed infants, identified as "Baby 1," "Baby Jones," or the like. The NBS laboratory has reported results to KY HIE under these placeholder names, and Kentucky's certified data analysts have later filled in the correct legal names — a tedious, time-consuming task entailing manually matching unnamed infant records with data from birth certificates, birthing centers, providers or parents.

Informatics Solution

The record-matching process now occurs automatically in the Kentucky Child System (KY Child), a "homegrown" information system that went live in 2006. In short, Kentucky's 52 birthing centers send to KY Child all newborn information. KY Child then pushes that information to the applicable state programs, such as the Kentucky Children with Special Health Care Needs program (for audiology results) and the Division of Laboratory Service (for information linked to the NBS specimen). The NBS specimen is sent to the laboratory with a requisition form and barcode matching the information uploaded to KY Child. Once a baby receives its legal name, typically by the seventh day postpartum, its birth certificate information is uploaded to KY Child. KY Child then transmits that information to the Kentucky Office of Vital Statistics and simultaneously updates all other records in the system linked to that infant.



Darrin Sevier, NBS supervisor, KY

Jacquelyn Lee, DPH, Kentucky's public health informatics manager, describes the state's "infrastructure house" thusly: "The foundation is the architecture, including the enterprise service bus that controls document management, the rules engine, master data management and security fraud analytics. The columns of the house are Kentucky Medicaid Services, the state health benefits exchange, support programs, public health programs, all-payers claims database and KY HIE. These columns hold up the roof: the state employees' portal and citizens' portal." KY HIE, said Lee, "is like a post office; it's a pass-through." When a credentialed provider queries KY HIE, it pings the servers housing patient data and sends that information back to the provider. A unique identifier links all information associated with each infant. "We want to be sure providers in Kentucky can query the KY HIE system for babies and find accurate information," Lee said.

(Note: As of April 2015, the system is not yet fully functional, and a redundant system is in place to assure timely notification of NBS results.)

Case Study 2: Sharing Environmental Test Data in New Jersey and Nationally

Background

New Jersey's Consumer, Environmental and Occupational Health (CEOH) Program — housed within the state Department of Health (DOH) — participates in CDC's Environmental Public Health Tracking Program, which integrates data about environmental exposures with data about diseases potentially linked to the environment.

Problem

To meet grant requirements, the CEOH Program needs to send CDC data detailing levels of specific analytes in community drinking water systems. This information, in turn, is collected by the New Jersey Department of Environmental Protection (DEP). Historically, DEP personnel have had to manually pull the data for each request, and, since the files are too big to send via e-mail or a standard web page, a DOH staff member has had to retrieve the data (stored on a thumb drive or CD) from DEP in person.

Informatics Solution

The CEOH Program is now able to access the data via the Environmental Information Exchange Network, a secure, national information network, which is a collaboration among US states, tribes, territories and the federal Environmental Protection Agency. The network has separate data flows for air, health, natural resources, waste and cross-program information. Each Exchange Network partner maintains its own data node and may specify who has access to what data on the node. Users can then extract the data they are authorized to access.

To implement the solution, DEP enlisted a vendor to tweak the EPA standard (in this case, the Safe Drinking Water Information System XML Schema) and to develop a software interface enabling CEOH Program personnel to pull the information they need, as they need it. In addition, CEOH Program staff can analyze retrieved data using a tool provided through the Exchange Network browser.

The informatics solution leverages existing tools and technologies and is efficient, elegant and user-friendly. DEP can approve access to additional analytes upon request. CEOH Program personnel can build customized queries — for specific date ranges, analytes, analyte concentrations, etc. — and the system maintains those queries for reference and re-use. And DOH and DEP personnel are no longer tasked with manually transferring the data.

"Build it once and use it often."
~ Mike Matso, New Jersey Department of Environmental Protection

IV. Legal and Procedural Considerations

To effectively implement shared services, laboratories need appropriate legal agreements in place and certain clearly delineated operational procedures and roles.

As with all business transactions, an established relationship with key negotiating partners — in this case the department or state chief information officer (CIO) — is beneficial. The textbox, "Get to Know Your Friendly, Neighborhood CIO," describes current state CIO priorities that may impact SLA negotiations.

The two core documents that need to be negotiated are the memorandum of understanding (MOU) and service level agreement (SLA). These are so critical to effective operations that the APHL Informatics Self-assessment Tool defines a maturity Level 3 laboratory as having formal agreements in place for all IT maintenance and support services.

Get to Know Your Friendly, Neighborhood CIO

Your state chief information officer (CIO) is a valuable asset whose job is to implement informatics solutions that support the government enterprise. It is useful for laboratory leaders to understand the CIO perspective on state IT services and to assure the CIO understands laboratory IT needs.

The National Association of State Chief Information Officers (NASCIO) — the professional membership association for state CIOs and US IT executives and managers — offers a plethora of information for those interested in the CIO perspective on IT developments or in state and national IT policies and trends, generally. For example, the website provides easy access to state IT strategic plans and organizational charts.

Top CIO priorities in 2014, according to NASCIO, include IT security, use of cloud services, strategic planning, cost control and use of wireless IT infrastructures and mobile IT products (including a trend toward BYOD – Bring Your Own Device). However, the #1 or #2 CIO priority for the past three years is the consolidation of IT services at the enterprise level.

For more information, visit www.nascio.org, and, of course, your own friendly, neighborhood CIO.

Memorandum of Understanding (MOU) — A High-level, General Agreement

APHL's 2011 report, *The Brave New World of Consolidated and Shared IT Services*, defines the MOU as a relatively high-level agreement describing broad concepts of mutual understanding, plans, goals and general roles of memorandum signatories. The report discusses eight potential MOU provisions, which we will not elaborate upon here:[9]

1. Prioritizing the LIMS as a critical adjunct to laboratory instruments and a core component of the laboratory infrastructure
2. Prioritizing the need for dedicated application-level LIMS support
3. Assuring 24/7 on-site IT support
4. Assuring laboratory authority to manage vendors
5. Addressing security clearances and protection of personal identifiers in laboratory data
6. Defining partnerships with high visibility agencies within the laboratory's government jurisdiction that have a governance role in IT affairs
7. Prioritizing IT support for emergency response activities
8. Assuring oversight and project management at the laboratory level

"We have lots of out-of-norm IT requirements for instruments, computers, etc. One of our big strategies is making sure we communicate effectively with what we call our IT relationship managers, making sure they understand the specific needs of our business operations and how best to roll out upgrades to make sure they don't cause service interruptions. . . . . Communication on the front end is very important."

Christopher L. Ball, PhD, HCLD (ABB)
Chief, Idaho Bureau of Laboratories

Service Level Agreement (SLA) — A Contract for Specific Services

In contrast to the MOU, the SLA is a more granular, contractual agreement defining a service commitment between two parties. It defines the service, costs of service delivery, contract terms and conditions, responsibilities of the parties and performance metrics (e.g., response times, recovery objectives, etc.). Often, it also details service incentives, as well as risks and penalties associated with failure to comply with agreement terms.

The SLA is a common, industry standard agreement. Typically, it incorporates specific **service level objectives** (SLOs) and, in fact, is sometimes referred to as a SLO document. SLOs, in turn, link specific shared informatics services to specific laboratory business operations and provide a rationale for the linkage.

Overall, the SLA provides laboratories a legal venue to delineate laboratory services, the internal and external informatics services needed to carry out those laboratory services, IT performance requirements, and business processes necessary to assure effective informatics service governance, including an ongoing review and annual approval process to make sure the SLA meets changing IT service needs. Importantly, the SLA can serve as a sharable template that interoperable PHLs can use to assure that informatics services align with information-sharing needs. For example, if ETOR is to be successful, every PHL node in the data exchange network must have certain assurances of IT support.

A typical SLA might include four straightforward sections (See Table 3).

A relatively brief **introductory section** includes:

- The purpose of the agreement (e.g., to identify services to be received by the state PHL, such as supporting the infrastructure upon which laboratory applications reside)
- Vendor goals (e.g., goals of state IT consolidation or technical justifications for exempting certain systems or applications from consolidation)
- The business background (e.g., the main business purpose of the systems being implemented and supported, such as using the LIMS to support laboratory workflows or messaging systems to facilitate data sharing with partners)
- Financial information, including available annual funds and funding sources for IT activities. It is important that the initial implementation and ongoing maintenance funds are identified
- A list of key business and technical contacts in the relevant IT office and in the laboratory
- A description of the responsibilities of each party in the agreement and the procedures to be followed should disputes arise as the suitability of the services being provided to fulfill the intended business needs
- A short statement describing how ongoing SLA updates will be initiated and approved, when needed

Table 3. Template for a Service Level Agreement

I. Introduction

- Background
- Business Background
- Financials
- Key Contacts
- Service Start Dates
- Future Updates to this SLA

II. Services Provided

- Services within the Scope of the SLA
- Service Start Dates
- Services beyond the Scope of the SLA
- Supporting Functions

III. Service Architecture

IV. Service Operations Procedure

- Incident Management
- Service Request Fulfillment
- Service Maintenance Windows
- Customer Notifications

The introduction is followed by a **description of the services to be provided**, including:

- A comprehensive list of all the services falling within the scope of the SLA, including technology services (e.g., network infrastructure or database services) and support services — in-scope services might include data back-up and recover activities (including schedules for incremental and full backups), database hosting, virtualized hosting services, maintenance of designated servers and applications (e.g., billing or electronic laboratory reporting applications) and security oversight, including compliance with enumerated federal security requirements
- Service start dates and uptime expectations, including identification of typical peak business hours during the normal workweek and any seasonal periods of heavy IT use
- A list of expectations describing the customer's role in maintaining IT services, such as daily operation monitoring or attending regular status update meetings — it is also important to identify any relevant services falling beyond the scope of the SLA that must either be provided internally by the laboratory or by a vendor or other entity
- A list of support functions for which the IT office is responsible, such as account management or project management.

Next is a series of diagrams depicting the **service architecture** and indicating:

- The physical location where specific systems reside
- The pertinent details regarding hardware to procured, such as processing power and the memory and disk space that will be made available
- The IP address topology of the systems deployed and the general routing schemes for network traffic (depicted in a network diagram)
- The structure of each software application being deployed and key interaction points between the modules and components (depicted in a system architecture diagram)
- The general structure of data being collected and stored (depicted in a high-level database diagram)

The final section describes procedures for key service operations:

- Expectations for resources that will be dedicated to incident response (often described in terms of the number of incidents expected during a period of time)
- Incident response procedures, including escalation of response times and resources based upon issue urgency
- Procedures for reporting an incident, including a mechanism to describe the incident priority level, based upon the degree to which it degrades or disrupts standard operations
- The mechanism that will be used to submit a service request, such as a request for changes to the system configuration or a request for software updates
- The system for prioritizing incidents and service requests (e.g., on a scale from low priority to catastrophic).
- Routine service maintenance windows and help desk hours
- Expectations for regular status meetings, including who should attend and a sample of a typical agenda
- Description of regular status reporting, perhaps in the form of dashboards, including content structure and identification of customer responsibilities to read and acknowledge the content
- Acceptable communication channels for external IT staff to use when notifying the laboratory of upcoming changes and possible service disruptions (e.g., by contacting specified staff)

> "In the era of laboratory consolidation, MOUs and SLAs are an absolute must. If IT staff don't have regular interaction with the laboratory, they do not understand the business process. And the business process of the laboratory is very different even from epidemiology. Ideally, you want IT staff dedicated to the lab. And you need to have it in writing."
>
> Bernd Jilly, PhD, MT(ASCP), HCLD(ABB)CC
> Chief, Alaska State Public Health Laboratories

To develop the SLA, laboratory leaders must identify agency IT service roles, as well as the responsibilities of laboratory IT staff. Agency-level services might include provision of firewalls and physical facilities, operating system and anti-virus software updates, hardware updates and improvements, ongoing system monitoring and 24/7 support. Laboratory-level responsibilities might include software licensing, application updates and database management functions. The more clearly the laboratory specifies its needs, the better.

V. Conclusion

Dramatic technological advances have made this an exciting time to be working in public health laboratory practice. Laboratories are now able to produce great volumes of accurate patient data and to collaborate with partners in ways that were inconceivable even a few years ago. However, the breadth and depth of IT hardware and services required to remain a player in today's public health ecosystem can be daunting. Thus, many PHLs will find it beneficial to create partnerships with external entities (e.g., vendors, other agencies within their governmental jurisdiction or private and public health partners at a national level) to obtain a significant chunk of their IT services. This new modus operandi will require a mix of managerial talent, organizational sophistication and technical acumen that must be built and fostered within our PHLs, if we are to succeed. We hope you find this document a useful starting point in your journey forward.

For more information on APHL's Informatics Program, visit www.aphl.org/informatics.

References

1. APHL. (2011). *The Brave New World of Consolidated and Shared IT Services: A Guide for Laboratories*. Silver Spring, MD: APHL. Retrieved from: http://www.aphl.org/AboutAPHL/publications/Documents/COM_2011_ITConsolidatedandSharedServices.pdf.

2. APHL. (2003). Requirements for Public Health Laboratory Information Management Systems: A Collaboration of State Public Health Laboratories, the Association of Public Health Laboratories and the Public Health Informatics Institute. Silver Spring, MD: APHL. Retrieved from: http://www.aphl.org/documents/global_docs/reqs_for_phlims.pdf.

3. Campbell A, Kunisch, S, Müller-Stewens G. (2011). To centralize or not to centralize? *McKinsey & Company*. Accessed June 28, 2013, from http://www.mckinsey.com/insights/organization/to_centralize_or_not_to_centralize.

4. APHL and CDC. (2013). Laboratory Efficiencies Initiative: Informatics Self-assessment Tool for Public Health Laboratories. Silver Spring, MD: APHL. Retrieved from: http://www.aphl.org/MRC/Documents/LEI_2013Jun_Informatics-Self-Assessment-Tool-for-PHLs.pdf.

5. Paulk MC, Weber CV, Garcia SM, et al. (1993). *Key Practices of the Capability Maturity Model*[SM], *Version 1.1*. Technical Report CMU/SEI-93-TR-025. Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute.

6. Baldwin R, State of Montana Chief Information Officer; personal communication, 5 May 2015.

7. Ibid.

8. Ibid.

9. APHL. (2011). *The Brave New World of Consolidated and Shared IT Services: A Guide for Laboratories*. Silver Spring, MD: APHL. Retrieved from: http://www.aphl.org/AboutAPHL/publications/Documents/COM_2011_ITConsolidatedandSharedServices.pdf.

Acknowledgements

The Informatics Committee would like to thank for following participants for their contributions to this white paper.

Special Thanks to Jack Krueger, MSChE, Emeritus Author:
The APHL informatics committee wishes to recognize the efforts of Jack Krueger in the production of this paper. After Jack retired as the laboratory director at the State Health Lab in Maine, he joined us as an extremely active member of the APHL informatics committee and contributed heavily towards most of products we have produced over the last several years. Without Jack, this white paper would not exist. Jack was not only the primary author and editor of the first Brave New World white paper, but he also recognized the need for this follow-up paper. As his last work before retiring from the committee, Jack worked tirelessly to recruit members of the informatics community help him to organize the initial drafts before handing it off to us to finish on his behalf. We therefore dedicate this white paper to Jack and publicly thank him for his dedication to the field of public health, and most of all, for the friendship and immense wisdom he shared with each of us on the APHL informatics committee.

Informatics Committee Computer Technology Needs Workgroup:

Martin R. Evans, PhD, CLT, MT(ASCP), APHL Senior Informatics Consultant, Global Health Program
Susanne Crowe, MHA, Laboratory Director, Jacksonville, Florida
Dari Shirazi, IT Director, State Hygienic Laboratory, University of Iowa
Frank Delin, Deputy Direct IT, State Hygienic Laboratory, University of Iowa
Stephen Soroka, MPH, LIMS Scientific Advisor and Coordinator, CDC
Eddie Gonzalez, MBA, PMP, CPHIMS, APHL Consultant, Uber Operations, LLC
Jack Krueger, MS, Retired Laboratory Director, Maine
Garrett Peterson, MBA, Incoming-Chair, Informatics Committee, Director of Life Sciences Technology, Yahara Software
Cassandra Hadley, APHL Staff Liaison, Informatics Committee

Member Laboratory Participants:

Christopher L. Ball, PhD, HCLD(ABB), Chief, Idaho Bureau of Laboratories
Ron Baldwin, CIO of Montana
Dina Caloggero, MPA, PMP, Director Informatics, Massachusetts State Laboratory
Mark Conde, Chair, Informatics Committee, Director, Information Technology, Emory/Rollins School of Public Health
Bernd Jilly, PhD, MT(ASCP), HCLD(ABB)CC, Laboratory Director, Alaska State Public Health Laboratories
Jacquelyn Lee, MS, Informatics Manager, Kentucky Department of Public Health
Nancy Maddox, writer, Maren Enterprises
Sharon P. Massingale, PhD HCLD/CC(ABB), Laboratory Director, Alabama Department of Public Health
Mike Matsko, NJ Department of Environmental Protection
Richard E. Opiekun, MA, MS, PhD, Environmental Data Coordinator, NJ Department of Health
James Smagala, PhD, SRA Project Manager, CDC Influenza Division

Association of Public Health Laboratories

The Association of Public Health Laboratories (APHL) is a national nonprofit dedicated to working with members to strengthen laboratories with a public health mandate. By promoting effective programs and public policy, APHL strives to provide public health laboratories with the resources and infrastructure needed to protect the health of US residents and to prevent and control disease globally.

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