Association Of Public Health Laboratories (APHL)
AIMS Frequently Asked Questions (FAQs)

History & Background

When and why was the AIMS Platform developed?
Initial development on the AIMS Platform began in 2007 under the name Route-Not-Read (RnR) Hub. The RnR hub eliminated the need to maintain multiple connections - one for each partner - to a single connection (see diagram below). The original use case was in support of the Public Health Laboratory Interoperability Project (PHLIP) focused on influenza reporting to the Centers for Disease Control and Prevention (CDC).

In 2012, the RnR Hub was renamed to the APHL Informatics Messaging Services (AIMS) Platform. Over the last few years, the capability has grown to encompass translation, transformation, and hosting in addition to the initial secure routing function.

Who works on the AIMS Platform?
The AIMS Platform is maintained by the Association of Public Health Laboratories (APHL) and the platform’s technical vendor, Ruvos. Approximately 50 people work together to secure, maintain, and enhance the
AIMS Platform. The team includes AWS certified professionals, security professionals, project managers, certified integration engineers, and vocabulary and terminology specialists.

Data & Users

Who are some of the trading partners on AIMS today?
Every state trades information via the AIMS Platform. Trading partners include public and private health laboratories, public health agencies, multiple programs at the CDC, and private hospitals and laboratories.

How does the CDC use the data that it receives?
The CDC program areas use the data for surveillance purposes. Much of the information gets compiled into data sets that provide an overview of current conditions throughout the United States.

How does the AIMS Platform support the initiatives towards Meaningful Use?
Many jurisdictions receive ELR data via AIMS to meet the Meaningful Use requirements. AIMS also supports an electronic case reporting program, which will assist providers and jurisdictions in preparing for Meaningful Use Stage 3.

Infrastructure

Where is AIMS hosted?
AIMS is hosted in the Amazon Web Services (AWS) cloud. Hosting locations for the AIMS infrastructure are in various regions and data centers throughout the United States. Fault Tolerance and High Availability are...
achieved by building a cloud-based infrastructure to take advantage of these multiple data centers. The AIMS infrastructure also uses AWS services that feature built-in, high availability, and fault tolerance protections (e.g. AWS RDS, S3).

I don’t know anything about cloud computing. Where can I find more information?
Cloud computing provides a simple way to access servers, storage, databases, and a broad set of application services over the Internet. A cloud services platform, such as AWS, owns and maintains the hardware required for these application services, while you provision and use what you need via a web application. Learn more about Cloud Computing from Amazon Web Services.

Region US-East-1 has 6 Availability Zones (data centers)
The AIMS Infrastructure is located entirely within the Continental United States.

What transport protocols are available on AIMS?
Only secure protocols are available for data transmission to and from AIMS. Supported protocols include Secure File Transport Protocol (SFTP), AWS S3, PHIN MS, Direct, and Web Services. AIMS also supports Virtual Private Network (VPN) for those partners that require it.

Can AIMS handle large file sizes and large volumes of messages/data?
AIMS is readily scalable and able to support transfers of virtually unlimited objects up to 5 terabytes each in size.

Security

Who controls and protects the data centers?
AWS is responsible for the control and security of the physical data center. They achieve this through physical barriers, access controls, video surveillance, and other methods that prevent unauthorized access. (Additional Information)

If AIMS is built on top of Amazon Web Services (AWS), who is ultimately responsible for security?
The AWS Shared Responsibility Model dictates which controls are AWS’ responsibility and which fall under the responsibility of the AIMS team. The AIMS team is responsible for those resources that sit in the cloud while AWS is responsible for the security of the cloud (e.g. physical hardware, hypervisor). (Additional Information)
Is the cloud a safe place to store and transmit data? Follow this link to see a list of AWS certifications and framework alignments. Beyond the extensive security controls in place at AWS, the AIMS platform frequently undergoes third-party penetrations tests, security audits, and robust disaster recovery exercises.

AIMS uses AWS S3 for transport and data storage. S3 is designed for 99.999999999% durability and up to 99.99% availability of objects over a given year.

For long-term storage, AIMS uses AWS Glacier, a highly durable storage infrastructure designed for long-term data archival and retrieval. It provides average annual durability of 99.999999999% for archives stored there. The service stores data in multiple facilities and on multiple devices within each facility to provide redundant copies of customer data. To increase durability, Amazon Glacier stores the data across multiple facilities before confirming a successful upload.

How do you keep my information safe? On top of AWS’ commitment to Data Privacy and Compliance, the AIMS security team uses various intrusion prevention systems and a range of security information and event management software to constantly monitor the FISMA Moderate environment.

What is HIPAA? What does AIMS do to adhere to HIPAA guidelines? HIPAA is the Health Insurance Portability and Accountability Act. While there is no certification for HIPAA for a cloud service provider, AWS does align its HIPAA risk management program with NIST controls, a higher security standard that maps to the HIPAA security guidelines. AIMS also undergoes frequent audits focused on ensuring HIPAA compliance.

The AIMS environment also has Business Associate Agreements in place with AWS as required by HIPAA rules. Only HIPAA eligible services are used within AWS to transmit, process, and store sensitive information.

For further compliance, the AIMS team undergoes FISMA audits of our environment built on AWS. This yearly assessment tests the controls we have in place to securely transmit data. (Additional Information)

Is AIMS compliant with FISMA, EHNAC, and other federal regulations? AIMS is hosted on AWS, a cloud service provider that meets FedRAMP, HIPAA, and Department of Defense compliance. FISMA adheres to NIST Special Publication 800 series and requires cloud service providers to undergo an independent security assessment conducted by a third-party assessment organization (3PAO) to ensure authorizations are compliant with the Federal Information Security Management Act (FISMA). AIMS was recently accredited by EHNAC and DirectTrust. EHNAC compliance establishes that Direct healthcare communications meet technical and legal standards for trust, security, and privacy. (Additional Information)
Does AIMS support two-factor authentications?
Yes, AIMS supports two-factor authentication, Single sign-on, and Identity Access Management.

Use Cases

What are some of the use cases on AIMS?
AIMS serves as a messaging platform that supports the transport of electronic lab results, data messaging between public health labs, whole genome sequencing data management and analyses, and much more. The AIMS platform is helping organizations meet Meaningful Use objectives, including national electronic case reporting initiatives. Use cases include:

1. PHLIP Flu
2. LIMSi
3. Vaccine Preventable Diseases (VPD)
4. NMI/MVPS
5. ELR from hospitals to jurisdictions
6. ELR from public and private laboratories to jurisdictions
7. Cross-jurisdictional ELR
8. NAPHSIS STEVE v2.0 Hosting
9. PHIZ Cross-jurisdictional Immunization Exchange
10. National Quest ELR Project to all jurisdictions across the United States
11. Whole Genome Sequencing via the Advanced Molecular Detection CDC program
12. Electronic Case Reporting (eCR) with RCKMS
13. Rabies Animal ELR from reference laboratories to the CDC
14. Emerging Infectious Program (EIP): FoodNet
15. Antibiotic Resistance Lab Network (ARLN)
16. Quest Diagnostics
17. Food and Drug Administration
18. COVID-19 reporting from public health laboratories/agencies to the CDC

Services Offered

What services are offered through the AIMS Platform?

Data Visualization Services
Applications, tools, and services available for the analysis and reporting of data on AIMS
• **Tableau** - Data Visualization and Business Intelligence Tool  
• **ElasticSearch** - Search and Analytics Engine  
• **QuickSight** - AWS data visualization tool  
• **Logstash** - Data Processing Pipeline  
• **Kibana** - Dashboards and Visualizations  
• **Grafana** - Metrics and Analytics Dashboard  
• **AIMS Custom Dashboards** - Secure dashboards to view metadata on messages flowing through AIMS

**Interoperability Services & Tools**  
*Services provided for trading partners focused on transport, translation, and transformation*

• **API Integration** - Software-to-software interface that allows for AIMS and trading partners to talk to each other with minimal effort.  
• **Single Sign-On and Identity Brokering**  
• **Route-Not-Read** - PHIN MS-based routing of encrypted data for recipients  
• **Mirth** - Integration Broker  
• **Intelligent Transport** - Automated interoperability between transport protocols.  
  o **Web Services** - Integration of Web-based applications using the XML, SOAP, WSDL, and UDDI open standards over an Internet protocol backbone.  
  o **SFTP** - Secure File Transfer Protocol  
  o **VPN** - Connection to AIMS via Virtual Private Network  
  o **S3** - Simple Storage Service. Fast, secure data transfer to AIMS.  
  o **PHIN MS** - CDC Messaging Platform  
  o **Direct** - Secure, Private Data Exchange between Trusted Recipients  
  o **IHE/NwHIN XDR**  
• **Intelligent Translation and Transformation** - Automated integration between file formats.  
• **Database Offerings** - DynamoDB, Redshift, MySQL, Oracle, SQL Server, Aurora, or PostgreSQL.  
• **Backup and Archiving** - Low-cost, highly reliable, and durable file storage.  
• **Disaster Recovery/Business Continuity** - Rapidly Recover Infrastructure and Data by leveraging 18 AWS Regions and 55 Data Centers.  
• **Git** - Code Repository and Version Control System

**Security Services**  
*Monitoring and Processes to ensure compliance with strict federal security standards*

• **Penetration Tests** - Vulnerability Assessments by 3rd Party Organizations
● **FISMA Audits** - Federal Information Security Management Act (FISMA) Independent Assessments
● **ENHAC** - The Electronic Healthcare Network Accreditation Commission
● **Adherence HIPAA Guidelines** - Business Associates Agreements, HIPAA Eligible Cloud Vendors and Services, HIPAA Training
● **SIEM / IPS Tools** - Deployed Security Tools and Services
● **NARFs** - Stringent, but streamlined Network Access Request Form process
● **AIMS Security, Monitoring, and Compliance** - Real-time monitoring, auditing, self-remediation, and protecting

**Hosting Services**
*Third-party and proprietary applications that are made available for AIMS trading partners*

- **Sara Alert** - Secure Monitoring and reporting for Public Health
- **RCKMS** - Reportable Conditions Knowledge Management System
- **STEVE** - State and Territorial Exchange of Vital Events
- **CELR** - CDC COVID-19 Electronic Lab Reporting (ELR)
- **PHIZ** - ONC Immunization Data Exchange
- **EIP** - CDC Emerging Infections Programs
- **DAART** - Data for Action on Antibiotic Resistant Threats
- **OpenELIS** - Laboratory Information Management System (LIMS)
- **Lab Web Portal** - Electronic Orders/Results Portal
- **NIST** - AIMS-hosted NIST validator

**How will using the AIMS Platform add value to my organization’s work?**

**Some of the advantages of using AIMS include:**

1. Open Source architecture
2. Centralized processing and message routing
3. Real-time monitoring and audit systems
4. Reduced message transport complexity
5. Reduced data translation and transformation complexity
6. Reduced development and support costs
7. Flexible capacity infrastructure
8. 5-year authentication certificates
9. Vocabulary and HL7 Message Support
10. Experienced and dedicated tech support
Customer Support

Is there a Help Desk for customer support? If so, how do I contact them?
You can email informatics.support@aphl.org. For emergency assistance, please contact 1-844-836-8377.

What if my organization is in need of additional technical assistance?
APHL has a robust Technical Assistance Program that is available to assist. (Additional Information)

I need a written document that provides an overview of the AIMS Platform. Where can I find one?
More resources on the AIMS Platform appear on the AIMS Platform resource page, including a One-Pager.

Are there educational resources related to AIMS?
Many resources are available through the AIMS Platform resource page. Educational videos are available at 2015 APHL Cloud Plenary and AIMS Overview at the 2016 Public Health Informatics Conference.

I'm interested in taking advantage of AIMS Platform services, what do I do next?
Please email us at informatics.support@aphl.org.