Sharing Success: AWS Transfer Family for SFTP Services

Abstract

Secure File Transfer Protocol (SFTP) has been leveraged in public health since the 2000s to exchange sensitive personally identifiable information (PII), such as medical records, securely and electronically between healthcare providers, organizations and public health agencies (Elliot et al., 2024). Outdated security infrastructure introduces substantial risks, especially in legacy services like SFTP.

In late 2023, the Association of Public Health Laboratories (APHL) weighed two options: 1) upgrade the legacy service to compliant SFTP or 2) transform the service to resilient AWS Transfer Family. APHL chose the latter, a transformation that would mean security and compliance would be actively managed externally by Amazon Web Services (AWS), leading to a solution that is auto-scalable, more efficient and more secure by modern standards. In this solution, all credentials would be self-managed.

The strategic APHL team was comprised of Project Management, Security Operations, Integrations Engineers, Production Operations and Service Delivery personnel. Through extensive cross-team collaboration and partnership, APHL completed the work to migrate approximately 65 partner organizations—including 19 eCR partners—during Q4 2024. Partners were given premium support to test their connectivity and ability to send a message. Proactive external communication ensured all parties were aware of project updates and received technical support. During the testing window, 60% of partners completed testing.

APHL's SFTP to AWS Transfer Family Migration occurred after-hours on January 14, 2025, with minimal interruptions. While approximately 15% of partners experienced minimal complications due to clean-up scripts originating from a single vendor's approach, issues were resolved the same day. Partners utilizing APHL's SFTP service will now be able to transfer data securely and efficiently with peace of mind in the resilience of the public health mission they serve.

Learn more about the AWS Transfer Family migration project and about APHL's support for electronic case reporting.

Sharing Success: AWS Transfer Family for SFTP Services

Introduction

Written by: Neal F Wolfe, MBA and Elena Jordanov, MPH

In response to security compliance requirements and the end-of-life (EOL) status of a Linux-based SFTP server, APHL chose to transform its services to meet modern-day security and management requirements through the migration to AWS Transfer Family. This transition involved migrating 65 known partners, including 19 eCR partners, to a more scalable, secure, and efficient infrastructure.

SFTP (SSH File Transfer Protocol, also known as Secure File Transfer Protocol) is a network protocol that allows for secure file transfer over a Secure Shell (SSH) connection. It is widely used to encrypt and protect data transfers between a client and a server. Unlike FTP, which transfers data in plaintext, SFTP encrypts both commands and data, ensuring secure transmission. SFTP has been leveraged in public health to exchange sensitive personally identifiable information (PII) securely and electronically, such as medical records, between healthcare providers, organizations, and public health agencies since the 2000s (Elliot et al., 2024). SFTP transport is easily attainable and commonly used, independent of platform. You can manually deploy SFTP, or you can use a client. Often, those who want to use S3 must go through a third-party to manage it, which is why SFTP is so highly leveraged in public health laboratories.

AWS Transfer Family is a fully managed service by Amazon Web Services (AWS) that provides secure file transfer capabilities using protocols like SFTP, FTPS, and FTP. AWS Transfer Family allows organizations to migrate and operate file transfer workloads in the AWS Cloud without managing any infrastructure. It integrates with Amazon S3 and Amazon EFS, making it ideal for scalable, cloud-native file storage solutions. AWS Transfer Family, being an SFTP-like transport, enables partners to leverage their existing transport method while also being technologically resilient to change.

Table 1: Comparison of AWS Transfer Family and SFTP (Amazon Web Services, 2025; Cusack et al., 2006; OpenBSD, 2025; Schlyter et al., 2006; Ylonen et al., 2001-2006)

Feature	AWS Transfer Family	Traditional SFTP Server
Storage Backend	Amazon S3 or EFS	Local disk or network storage
Infrastructure Management	Fully managed	Requires setup and maintenance
Scalability	Automatically scales	Limited by server capacity
Authentication	IAM, SSH keys, custom auth	Local user management or LDAP
Automation	Event-driven via Lambda	Manual or cron jobs
Cost Structure	Pay-as-you-go (usage-based)	Fixed hardware and maintenance costs
Security & Encryption	Data encrypted via AWS KMS, SSH keys	Data encrypted via SSH keys or TLS
Logging & Monitoring	CloudWatch, CloudTrail integration	Syslog or third-party logging tools
Multi-Protocol Support	Supports SFTP, FTPS, FTP	Typically supports only SFTP unless configured otherwise
High Availability	AWS manages redundancy and uptime	Requires manual failover or clustering setup

Custom Integrations	API-driven and Lambda-based automation	Requires scripting or third-party tools
Network Access Control	AWS Security Groups, VPC control	Firewall rules, VPN, private network

Implementation

APHL is a leading organization in national public health surveillance and informatics technical assistance. We are dedicated to accelerating time-consuming reporting obligations by utilizing the extensive technical expertise and capabilities of our laboratory subject matter experts and IT administrators. This support benefits healthcare organizations as well as state, tribal, local and territorial (STLT) jurisdictions.

The strategic APHL team includes experts from Project Management, Security Operations, Integration Engineering, Production Operations and Service Delivery. The team worked collaboratively in a safe and respectful environment. Project issues were skillfully discussed to successfully align understandings and best approach with the impacted teams and partners. Through extensive cross-team collaboration and partnership, APHL completed the work to migrate approximately 65 partner organizations—including 19 eCR partners—during Q4 2024.

The project scope began with the full intent of being a transparent migration, a logical swap of one infrastructure for another; however, it quickly expanded during the discovery and planning phase. The final scope included:

- Credential and contact management via the Cognito module,
- RSA key management,
- FISMA standards and enforcement of modern ciphers and encryptions,
- Data management and migration.

Partnership and Outcomes

Clear and up-to-date communication with partners was a key tenant of this project, allowing 60% of partners to successfully test connectivity and data sharing during the testing window. Emails were delivered to all known project partners to outline project scope and timeline, set partner expectations, share testing instructions, and communicate ongoing project updates. All information was readily available in an external Confluence space for partners to readily access and review real-time updates.

The APHL Team leveraged the knowledge and connections of all APHL Program Leads as this migration to AWS Transfer Family impacted partners in all programs, including eCR, Datapult, PHLIP, and more. Thanks to the collaboration and preparation of the team and our partners, all trading partners were successfully migrated, and no system-wide issues occurred.

At the end of the project, partners were invited to complete an optional Project Close Out Survey, which reflected an overall positive experience with this migration. Please find the survey results below.

Table 2: SFTP Migration Project Close Out Survey Results

Project Component	Survey Result
Overall experience	Great – Excellent
Access to technical experts	Great – Excellent
Timelines/Meetings	Great – Excellent
TA Process/Expectations	Great – Excellent

Access to useful guidance materials	Good – Excellent

Opportunities for the Future

While this project was technical in nature, a prominent challenge was creating a key parties registry to encompass all contacts within an entity—even in cases where separate entities operated within the same state partner. The Cognito module implemented through this project streamlines Identity and Access Management (IAM). IAM naturally provides a structured listing of users and contact details. With the self-service functionality of Cognito, users can now actively maintain their own information, ensuring accuracy and relevance. By placing control in the hands of the customer, self-service enables seamless updates and communication. Additionally, APHL can leverage this tool to direct updates and messages to a designated mailbox for streamlined correspondence.

Future APHL projects will prioritize collaboration with the APHL Service Delivery team to ensure timely communication about system maintenance windows and prompt identification and resolution of issues.

This project was made possible through the hard work of staff at APHL, Ruvos and J Michael Consulting.

References

Amazon Web Services. (n.d.-a). What is AWS Transfer Family? AWS Transfer Family User Guide. Retrieved March 13, 2025, from: https://docs.aws.amazon.com/transfer/latest/userguide/what-is-aws-transfer.html

Amazon Web Services. (n.d.-b). AWS Transfer Family pricing. AWS Pricing. Retrieved March 13, 2025, from: https://aws.amazon.com/aws-transfer-family/pricing/

Cusack, F., & Forssen, M. (2006). Generic Message Exchange Authentication for the Secure Shell Protocol (SSH) (RFC 4256). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4256

Elliot, A. J., Hughes, H. E., Harcourt, S. E., Smith, S., Loveridge, P., Morbey, R. A., Bains, A., Edeghere, O., Jones, N. R., Todkill, D., & Smith, G. E. (2024). From Fax to Secure File Transfer Protocol: The 25-Year Evolution of Real-Time Syndromic Surveillance in England. Journal of medical Internet research, 26, e58704. https://doi.org/10.2196/58704

OpenBSD Project. (n.d.). sftp-server(8) manual page. OpenBSD manual pages. Retrieved March 13, 2025, from https://man.openbsd.org/sftp-server.8

Schlyter, J., & Griffin, W. (2006). Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints (RFC 4255). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4255

Ylonen, T., & Lonvick, C. (Eds.). (2006). The Secure Shell (SSH) Transport Layer Protocol (RFC 4253). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4253

Ylonen, T., & Lonvick, C. (Eds.). (2006). The Secure Shell (SSH) Connection Protocol (RFC 4254). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4254

Ylonen, T., & Lehtinen, S. (2001). SSH File Transfer Protocol (Internet-Draft No. draft-ietf-secsh-filexfer-02). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-ietf-secsh-filexfer-02 Note: Internet-Drafts, such as draft-ietf-secsh-filexfer-02, are working documents of the IETF and are considered "work in progress." Therefore, they may not have the same authoritative status as published RFCs.