## Kitewcrks

# Kiteworks Platform

Federal Agency and Contractor Customer Stories



## Zero Visibility. No Control. High Risk.

Every day, federal agencies and contractors risk data breaches and compliance violations when they share CUI, IP, PII, PHI, and other sensitive data with citizens, suppliers, other agencies, and external partners using applications designed for expediency over security. But complex digital supply chains and IT infrastructure make it very difficult to protect these risky third-party communications from today's sophisticated, persistent threat actors that are patiently searching for your weakest link.

Kiteworks helps IT executives lock down the exchange of confidential enterprise information with digital supply chain partners by unifying security and compliance across siloed third-party communication channels, including email, file sharing, mobile, chat, web forms, managed file transfer, and SFTP. Chief information officers (CIOs), chief information security officers (CISOs), and chief risk officers throughout the government, as well as contractors around the country, trust the Kiteworks platform to provide their organizations with protection, privacy, and peace of mind.

# How the Kiteworks Platform Works

## SEE SENSITIVE DATA COMING AND GOING

#### Monitor Sensitive Files Shared With Customers, Suppliers, and Partners

on the CISO Dashboard or on your SIEM. Get a full picture of what content is being shared, where it is going, who is accessing it, when it happens, and how it is done. The Kiteworks platform produces a single, normalized syslog that lays the foundation for threat detection, response, and forensics.

. . . . . . . . . . . . . .

## 01

### CONSOLIDATE RISKY COMMUNICATIONS

#### Consolidate and Control Risky Third-party Communications

across email, file sharing, managed file transfer, web forms, and application programming interfaces (APIs) by routing each channel through the Kiteworks platform. Protect your sensitive data more simply, centrally, and uniformly with every channel you add. Save money while securing your business by eliminating legacy apps.

## SIMPLIFY SECURIT

. . . . . . . .

## Protect Data With Uniform Security and Compliance

across communication channels.
Define policies centrally for the
Kiteworks platform to enforce as it
inspects each transaction. Employ
FIPS 140-2 Validated encryption and
FedRAMP Moderate Authorized or
100% on-premise deployments and
send each data exchange down a
gauntlet of security, including SSO,
MFA, AV, ATP, and DLP, with a
single point of integration. Prove
compliance with a detailed audit
trail.



## Agency Collects Nationwide Epidemiology Reports in Compliance

Replaces Noncompliant Portal With Secure HIPAA-compliant Uploads

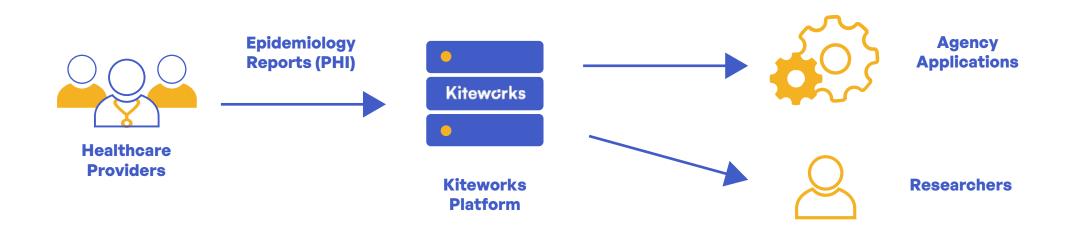
This critical agency collects infectious disease reports from thousands of medical personnel in virtually every public and private medical organization across the country. It feeds over one hundred applications at the heart of American epidemiology: analytics, research databases, statistical tracking systems, and many others. Unfortunately, tightening regulations had rendered its home-grown collection system out of compliance. The system must preclude doctors from seeing each other's submissions, laden with personally identifiable information (PII) and protected health information (PHI). As for the applications, the collection system must enforce data access levels managed in a central LDAP system.

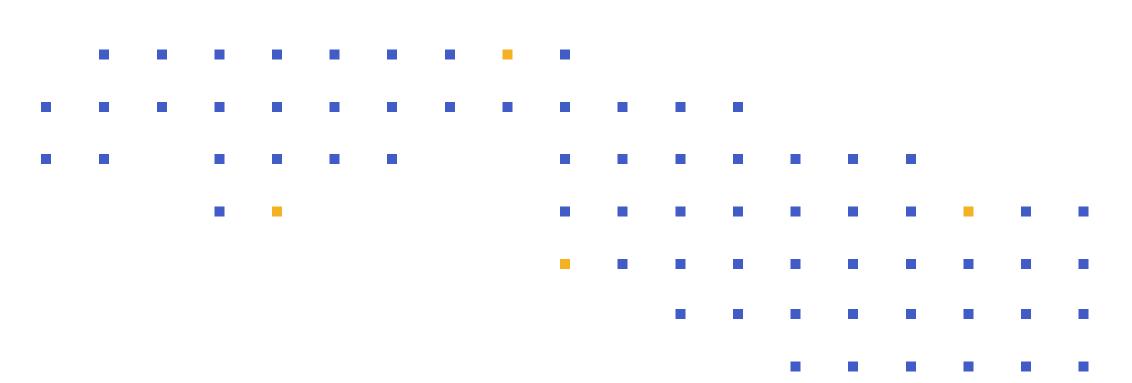
The integration team implemented multiple high-availability Kiteworks instances, each enabled by a different data access level specified in LDAP.

The Kiteworks platform provided the security, scale, immutable audit trail, and reliable data transfer functionality, including shared web folders and SFTP.

This freed the developers to focus on the custom REST API integrations for the legacy applications, meeting a break-neck schedule without risking a process essential to the nation.

A major agency securely collects infectious disease report uploads from the nation's healthcare providers and automates transfers to hundreds of tightly governed back-office applications.





## **Department Achieves Compliance** for Overseas Health Records

Secures Local Health Care Provider Transfers While Providing **Comprehensive Audit Trail** 

This department's employees work in locations around the world, and frequently use local health services. The department handles records in Washington, however, which led to a failed compliance audit for its protected health information (PHI) transfers. Local doctors and nurses needed a HIPAA-compliant way to send and receive health histories and other medical records. Importantly, these external parties had to use it without training—it had to be completely intuitive—and local employees had to securely manage them in time zones far from the administrators.

Kiteworks delivers a private content network for the department via Kiteworks FedRAMP. It provides easy-to-use secure uploads and email with worldwide reach, with secure invitations that make self-service management of external users a snap. The administrators, meanwhile, control the security policies and roles via its web console back at home, and make use of its comprehensive audit trail and reporting for audits.



**Uses Secure Shared Folders and Email to Protect Evidence** 

**Department's OIG Maintains CJIS** 

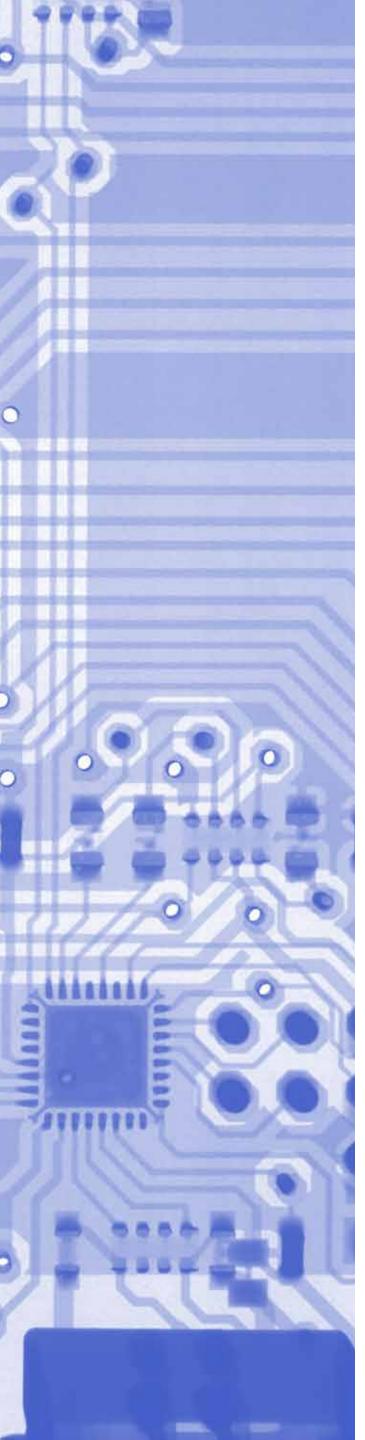
Agents must take extra precautions to preserve and protect evidence when their investigations cross the jurisdictions of states and foreign governments. By law, they are required to include these other organizations, and they often cooperate to bring down major fraud rings. But they need the right tools to share evidence while upholding the FBI's CJIS requirements, hand it off to law enforcement, and make the conviction stick.

This office began using Kiteworks FTA a decade ago for secure email and sharing of evidence leading to over \$1B in fraud convictions. They moved to the Kiteworks platform to meet new policies for SSO with PIV/CAC cards, stronger security controls, onboarding foreign agents without the need for training, and secure external sharing of files in Microsoft OneDrive®.





www.kiteworks.com



# **Dispute Resolution Office Digitizes Privacy-sensitive Workflow**

Delivers Compliant Cloud-based Submission and Case Management

This government agency needed to modernize its process for handling employee whistleblower and harassment cases, as mandated by Congress. It had to move from paper to the cloud, and with such sensitive data—and so many communications with the involved parties—it needed tight privacy and access controls. The agency was also subjected to frequent compliance audits, and wanted to streamline them with easy access to end-to-end activity logs. The team faced challenges in providing a secure and governed employee portal, data communications, file access, and case flow management.

They met these challenges by building on the Kiteworks platform. Its security by design and built-in settings provide the necessary user and data governance controls, file communications, and secure case folders, while its FedRAMP option side-steps the lengthy cloud authorization process. Its comprehensive logging and reporting streamline audit preparation. Straightforward REST API integrations with Microsoft Forms and a case management system complete the solution. It has won quick user acceptance with its easy-to-use interfaces for submitters, stakeholders, and case workers, not to mention the compliance and administration staff.



#### Step 1

Employee files dispute form

This dispute resolution office ensures employee harassment and whistleblower cases stay organized and completely private from the initial submission, through communications with the affected parties to decision-making and final archive.

#### Step 2

Case administrator receives notification and begins managing case

#### Step 3

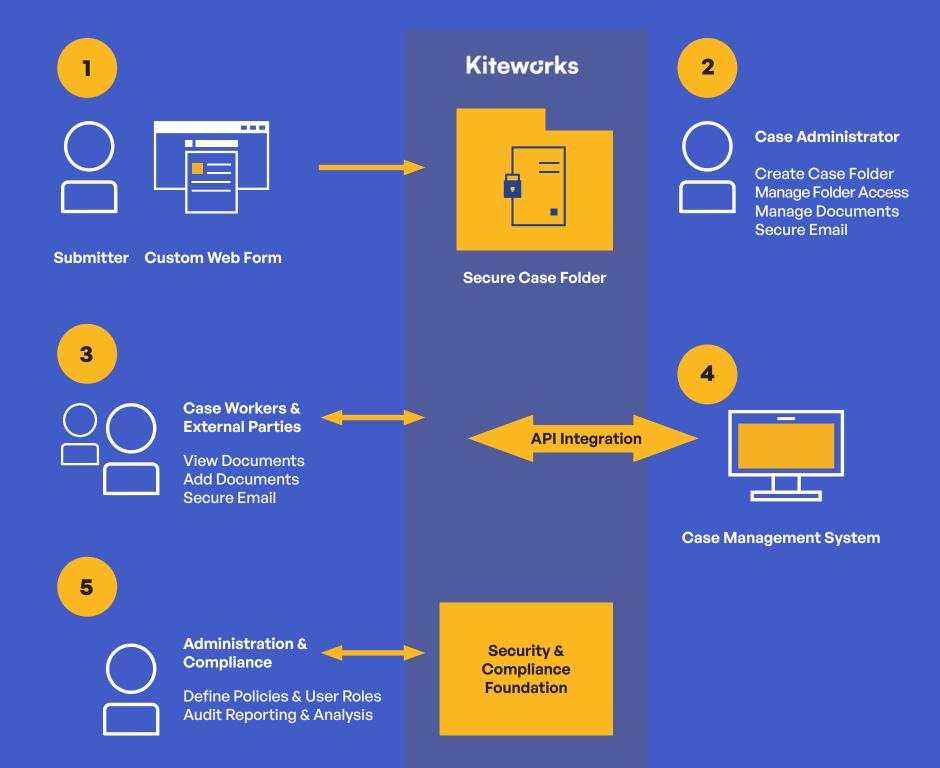
Arbitrators, managers, and affected parties review and submit documents

#### Step 4

Case management system receives final records via API

#### Step 5

IT administers users and policies; compliance manager handles audits





# Kitewcrks

www.kiteworks.com March 2022

Copyright © 2022 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.







