

PRIVATE HEALTHCARE · LGPD COMPLIANCE · BRAZIL

How Care Plus Made DLP Enforcement Work Without Blocking Users

A private healthcare operator in São Paulo migrated from a self-managed on-premises deployment to Kiteworks SaaS — integrating corporate DLP redirect, large file transfer, and automated SFTP for 3,000+ external users under a single governance layer.

SECURE EMAIL

DLP INTEGRATION

SFTP/MFT

LGPD

LARGE FILE TRANSFER

SAAS/HOSTED

About Care Plus

Care Plus is a private healthcare operator headquartered in São Paulo, Brazil, with a network spanning internal clinical and administrative staff, strategic partner organizations, patient representatives, and external providers. Operating under Brazil's LGPD data protection framework, Care Plus must demonstrate accountability for how sensitive data moves — who sent it, who received it, and whether access was appropriate. For years, the organization ran Kiteworks on-premises. The platform did the job. Running the infrastructure did not.

THE CHALLENGE

Self-managed infrastructure, no governed path for sensitive outbound email

What wasn't working

Running Kiteworks on-premises put the full operational burden on an IT team whose purpose was to govern data exchange, not operate a data center. Patching, capacity planning, and uptime were constant overhead. Meanwhile, corporate DLP policy had no reliable governed path for flagged outbound email. When a message triggered a DLP rule, the only choices were to block it or let it through — blocking frustrated staff and drove workarounds; allowing it left no audit trail. Neither option satisfied LGPD's accountability requirements.

What Kiteworks delivered

Care Plus migrated to Kiteworks SaaS, transferring infrastructure responsibility entirely. The DLP integration was configured to redirect flagged outbound email into Kiteworks Secure Email rather than blocking it — sensitive data moves through an encrypted, policy-governed channel and every transfer is captured in a tamper-evident audit trail. Large files that cannot transit standard email — medical imaging, diagnostic reports, audit packages — are exchanged through the same control plane for secure data exchange. More than 3,000 external users participate in governed exchange without consuming internal licenses.

HOW IT WORKS

DLP redirect — governed at the policy layer, not by procedure

When a user's outbound message triggers corporate DLP, policy redirects them to Kiteworks Secure Email rather than blocking the send. Every transfer is encrypted, logged, and auditable. Standard messages flow normally — no friction for routine communications.

1

DETECT

DLP Flags Sensitive Data

Corporate DLP scans outbound messages for sensitive data — patient records, medical reports, regulatory filings. A redirect action is triggered on match.

2

REDIRECT

User Routes to Secure Email

The sender is pushed to Kiteworks to complete the send. Message and attachments transmit over an encrypted, policy-governed channel — no blocked workflow.

3

DELIVER

Recipient Accesses Securely

Partners, providers, and patient representatives retrieve data through the Kiteworks external portal. No internal license required for external recipients.

4

AUDIT

Every Transfer Logged

File-level records capture sender, recipient, timestamp, and access events — the accountability evidence LGPD requires, without custom reporting.

PLATFORM CAPABILITIES

One governance layer — across every data movement channel

**Secure Email With DLP Integration**

Corporate DLP policy redirects flagged outbound email into Kiteworks. Approximately 90% of all platform activity runs through this flow — the primary daily use case.

**Large File Transfer**

Medical imaging, diagnostic reports, audit packages, and contracts that exceed standard email limits move through Kiteworks — off consumer tools and personal drives.

**External User Portal**

3,000+ partners, providers, and patient representatives participate in governed data exchange using downloader and uploader roles — none consuming internal licenses.

**Automated SFTP Exchange**

One strategic partner integration runs on automated, SSH key-authenticated SFTP under the same governance layer as all other data movement — consistent policy, one audit trail.

**LGPD-Ready Audit Trail**

Tamper-evident file-level logs capture every send, receive, and access event. Care Plus IT produces LGPD accountability evidence directly from the admin console.

**Self-Service IT Administration**

User provisioning, life-cycle management, and capacity monitoring are handled entirely by Care Plus IT through the admin console — no external support engagement needed.

USE CASES

Four governed exchange patterns — all under one policy layer

1

DLP-Redirect Secure Email

Corporate DLP redirects flagged outbound messages to Kiteworks Secure Email rather than blocking them. Users complete the send through a governed, encrypted channel — roughly 90% of daily platform activity flows through this path.

2

Large File Sharing

Medical imaging studies, diagnostic reports, audit packages, and contract bundles that exceed standard email limits are exchanged through Kiteworks — eliminating the fallback to consumer file-sharing tools and personal drives.

3

External Partner Network

3,000+ partners, providers, and patient representatives participate in governed data exchange using downloader and uploader roles. Care Plus extended its governance perimeter across the entire partner network without adding per-seat licensing cost.

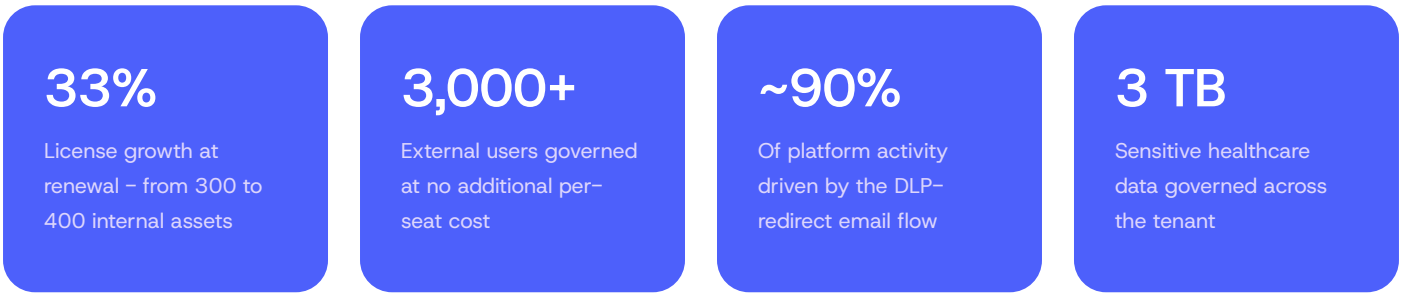
4

Automated SFTP Integration

One strategic partner runs automated, SSH key-authenticated SFTP file exchange under the same governance layer as the rest of the platform — consistent policy enforcement, unified audit trail.

RESULTS

Operational from day — growing at renewal



Needs addressed	Kiteworks capabilities deployed
✓ Eliminate on-premises infrastructure overhead – shift from self-managed server to governed SaaS	✓ Kiteworks SaaS (Hosted) — fully managed, zero on-premises infrastructure
✓ Governed path for corporate DLP-flagged outbound email — redirect rather than block	✓ Secure Email with corporate DLP integration — redirect, not block
✓ Large file exchange for medical imaging, reports, and audit packages outside standard email limits	✓ Large file transfer – governed, encrypted, auditable for medical and operational data
✓ Extend governance to 3,000+ external users without per-seat license cost	✓ External user portal with downloader/uploader roles – 3,000+ users, no license consumption
✓ Automated SFTP partner exchange under consistent policy governance	✓ SFTP with SSH key authentication for automated partner data exchange
✓ Tamper-evident audit trail for LGPD accountability — no custom reporting layer	✓ Tamper-evident file-level audit trail across all channels — email, file sharing, and SFTP

Copyright © 2026 Kiteworks. Kiteworks’ mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.