Kiteworks

COMPLIANCE BRIEF

Secure Pharmaceutical Systems for GxP EudraLex Annex 11 Requirements

Validate and Secure Pharmaceutical Data Systems in the European Union

EudraLex Volume 4, Annex 11 establishes requirements for computerized systems used in pharmaceutical manufacturing across the European Union, affecting both human and veterinary medicinal products. The European Commission published this regulation to ensure computerized systems maintain product quality, process control, and quality assurance without increasing operational risks. The directive took effect June 30, 2011, requiring pharmaceutical companies to validate all applications and qualify IT infrastructure. The regulation mandates specific controls for data integrity, system security, electronic signatures, and business continuity. Companies must implement comprehensive risk management throughout each system's life cycle while maintaining detailed documentation and audit logs. Noncompliance with Annex 11 can lead to regulatory action under Directives 2001/83/EC (human medicines) and 2001/82/EC (veterinary medicines), potentially resulting in manufacturing suspension, product recalls, or loss of manufacturing authorization in the EU market. Kiteworks supports these requirements. Here's how:

System Validation Through DevSecOps and Hardened Virtual Appliance Controls

EudraLex Annex 11 requires pharmaceutical companies to validate their computerized systems and maintain rigorous controls over data processing and system availability. The regulation mandates that organizations validate all applications, qualify IT infrastructure, implement secure data entry checks, and establish business continuity measures—all without compromising product quality or increasing operational risks when replacing manual processes. Kiteworks is committed to securing sensitive information with ISO 27001 guidelines and investments in security governance, processes, and controls.
With enhanced risk assessment and mitigation processes, regular internal and external penetration testing, an ongoing bounty program, and audits for SOC 2, FedRAMP, and other regulations, Kiteworks ensures the protection and privacy of information assets.
The DevSecOps "Shift Left" process validates system security through comprehensive training, design reviews, code analysis, and OWASP-compliant penetration testing.
The hardened virtual appliance protects data integrity using layered security controls including an embedded network firewall, web application firewall, and zero-trust architecture for secure data processing. For business continuity, Kiteworks provides high-availability clustering, cryptographically verified system updates, and secure offline updates for air-gapped environments. These features create a validated, secure environment that maintains data integrity while ensuring system availability.

Solution Highlights

- Comprehensive audit logs
- SIEM integration
- Hardened virtual appliance
- Double encryption
- Role-based access controls
- Multi-factor authentication

Data Storage and Archival Security With Double Encryption Protection

Strict requirements for securing and preserving pharmaceutical data throughout its life cycle requires organizations to protect data from both physical and electronic damage while maintaining its accessibility, readability, and accuracy. Companies must implement regular backup procedures and verify data integrity during validation and archival phases. Kiteworks supports these requirements through its comprehensive encryption and data protection features. The system employs file and disk double encryption, which applies separate encryption keys at both the file and disk levels, providing two distinct layers of cryptographic protection. The single-tenant private cloud architecture isolates each customer's databases, file systems, and application runtimes to prevent unauthorized access. For long-term archival, Kiteworks maintains data integrity through comprehensive audit logs while preserving the double encryption protection, ensuring archived data remains secure, accessible, and verifiable even as systems change over time.

Access Control and Documentation Using Role-based Controls and Audit Logging

Organizations are to employ strict access controls and documentation requirements for pharmaceutical operations, particularly focusing on batch release processes, security authorizations, data accuracy, and printed records. The regulation requires clear identification and authentication of qualified persons, comprehensive access controls, validated data entry processes, and verifiable printed records that show modification history. Kiteworks implements these requirements through multilayered security features. Role-based access controls with least-privilege defaults restrict system access to authorized personnel, while certificate-based authentication and multiple authentication methods (MFA, SAML 2.0 SSO, Kerberos, OAuth) ensure secure user verification. The content-based risk policies framework enforces dynamic controls based on content attributes and user actions and comprehensive audit logs maintain detailed records of all system activities, including file modifications, access authorizations, and timestamps.

System Documentation Through Comprehensive Audit Logs and Change Monitoring

Pharmaceutical organizations are to maintain comprehensive validation documentation, audit logs, and change management controls throughout their computerized systems' life cycles. All system modifications, configurations, and deviations must be documented with clear reasoning and remain traceable and reviewable. Kiteworks meets these requirements through its comprehensive audit logs system, which captures and retains all security and compliance-related activities in real time. The logs automatically clean, normalize, and aggregate data into a standardized format, ensuring consistent documentation of all system changes and user actions. The built-in CISO Dashboard and SIEM integration make these logs readily accessible and intelligible. The embedded MDR monitors system modifications while the no admin access feature prevents unauthorized changes to files, software, or configurations without proper authorization and documentation, maintaining system integrity and traceability.

Kiteworks provides pharmaceutical organizations with a comprehensive platform that aligns with EudraLex Annex 11 requirements through integrated security, validation, and documentation features. The Kiteworks Private Content Network is certified for ISO 27001, 27017, and 27018. The certifications ensure information confidentiality, integrity, and availability. Kiteworks features 175 validated controls and secure deployment options including a single-tenant architecture to protect organizations against cyber threats. The platform's DevSecOps approach ensures continuous system validation while the hardened virtual appliance creates multiple layers of security protection. The file and disk double encryption system safeguards data throughout its life cycle, from active use to long-term archival. Role-based access controls and diverse authentication methods restrict system access to authorized personnel, while content-based risk policies enforce dynamic security controls based on specific data attributes. The audit logs maintain complete documentation of all system activities, changes, and user actions, providing pharmaceutical companies with the detailed tracking and validation evidence required for regulatory compliance.

Kiteworks

November 2024

www.kiteworks.com