The Evolving Landscape of Pharmacovigilance IT: Key Considerations for the EU Regulation Amendment

Introduction

The European Commission's draft amendment to Implementing Regulation (EU) No 520/2012 introduces significant updates to pharmacovigilance activities, with far-reaching implications for IT quality assurance in the pharmaceutical industry . As organisations prepare for these changes, they face critical decisions about implementing robust IT governance frameworks that extend well beyond computer system validation (CSV) to include data governance, data integrity, and comprehensive audit strategies.

The Expanding Scope of IT Quality in Pharmacovigilance

The proposed regulation brings several important modifications that broaden the IT quality considerations for pharmacovigilance systems:

Enhanced Third-Party Accountability and Audit Requirements

The amendment significantly strengthens requirements for subcontractor oversight, stating:

"Where the pharmacovigilance tasks have been subcontracted by the marketing authorisation holder to a third party (or by this third party to another third party), delegation arrangements, each party's responsibilities, and audit and inspection arrangements should be clearly documented."

This necessitates:

- Comprehensive audit programs extending across organisational boundaries
- Documented audit trails for data exchanged between organisations
- Clear delineation of data ownership and governance responsibilities
- Formal information security assessments of third parties

Risk-Based Quality System Audits

The regulation places greater emphasis on audit processes, specifying:

"Marketing authorisation holders shall perform regular audits of the quality system at risk-based intervals to ensure that it complies with the requirements [...] and to determine its effectiveness."

Organisations will need to develop:

- Structured audit methodologies targeting high-risk processes
- Evidence of audit trail review and integrity verification
- Documented assessment of system security controls
- Proactive audit planning based on risk assessment outcomes

Computer System Validation in Context

While computer system validation remains essential, the amendment positions it within a broader IT quality framework. Critical CSV considerations include:

- **Documented Risk Assessment:** Formal evaluation of system impact on patient safety
- **Requirements Traceability:** Clear mapping between regulatory requirements and system functionality
- **Configuration Management:** Controls ensuring validated state is maintained during updates
- **Testing Strategy:** Risk-based approach focusing on critical system functions
- **Ongoing Fitness Verification**: Regular review of systems' continuing suitability

Data Governance and Integrity Requirements

Beyond CSV, the regulation implicitly demands robust data governance through:

- **Data Life Cycle Management:** Policies for data acquisition, processing, storage, and archiving
- **Data Quality Controls**: Procedures ensuring accuracy, completeness, and consistency
- **Audit Trail Functionality:** Comprehensive history of data creation, modification, and deletion
- **Access Management:** Role-based controls limiting data manipulation
- **Data Integrity Monitoring:** Active surveillance of data quality metrics

The Value of Comprehensive IT Quality Approaches

Successfully implementing these requirements demands expertise across multiple IT quality domains. Organisations with mature IT quality assurance programs generally benefit from balanced implementation approaches:

For Organisations with Limited Resources

- Develop risk-based audit schedules focusing on critical processes first
- Implement data governance frameworks that scale with organisational growth
- Create streamlined data integrity policies addressing essential ALCOA+ principles
- Conduct targeted CSV activities on highest-risk systems while developing broader governance
- Leverage industry templates for audit checklists and data integrity assessments

For Organisations with Established PV Systems

- Integrate audit functions across quality management systems
- Implement automated data governance monitoring where feasible
- Conduct comprehensive data integrity assessments across the PV data lifecycle
- Refine existing audit programs to incorporate third-party oversight
- Develop metrics to evaluate audit effectiveness and drive continuous improvement

Audit Strategy Development

Regardless of organisation size, a robust audit strategy should include:

1. **Risk-Based Planning**: Prioritising audit resources based on process criticality and system impact
2. **Multi-Dimensional Scope**: Covering systems, processes, data, and third parties
3. **Clear Audit Standards**: Developing specific criteria for evaluating compliance
4. **Root Cause Analysis**: Identifying underlying causes rather than symptoms
5. **Audit Program Metrics**: Measuring effectiveness of the audit process itself
6. **Escalation Protocols**: Defined processes for critical findings
7. **Knowledge Integration**: Mechanisms to incorporate learnings from each audit

Case Studies

Case Study 1: Subcontractor Management

The amendment specifically requires third parties to "agree to be audited by or on behalf of marketing authorisation holders and inspected by the competent authorities."

A balanced implementation approach includes:

1. **Contract Review**: Analysing existing agreements against new requirements
2. **Risk-Based Assessment**: Prioritising vendors based on criticality to pharmacovigilance
3. **Technical Controls**: Implementing appropriate system controls for third-party access
4. **Documentation Strategy**: Developing proportionate documentation with clear vendor responsibilities
5. **Audit Planning**: Creating a risk-based audit schedule matching vendor criticality
6. **Stakeholder Engagement**: Involving key stakeholders from compliance, legal, and IT

Case Study 2: Eudravigilance Database Monitoring

A mid-sized pharmaceutical company needed to implement enhanced Eudravigilance database monitoring per the requirement: "Marketing authorisation holders shall monitor the data available in the

Eudravigilance database together with data from other available sources, as part of their pharmacovigilance responsibilities."

Their approach featured:

1. **Signal Detection Framework**: Development of a structured framework combining automated and manual review processes
2. **Integration Strategy**: Connecting Eudravigilance data with internal safety systems and literature monitoring
3. **Analytical Tools**: Implementation of statistical analysis tools to identify emerging trends
4. **Validation Protocol**: Creation of a risk-based validation strategy focusing on algorithm reliability
5. **Process Documentation**: Development of SOPs with clear decision trees and accountability
6. **Performance Metrics**: Establishment of KPIs to monitor the effectiveness of signal detection
7. **Training Program**: Comprehensive training for pharmacovigilance staff on the new monitoring processes

This structured approach allowed the company to demonstrate compliance while enhancing their signal detection capabilities. Their implementation balanced automation with human expertise, ensuring technology augmented rather than replaced scientific evaluation.

Case Study 3: International Standards Implementation

A global pharmaceutical organisation faced the challenge of implementing international standards as required by the amendment: "In order to facilitate the interoperability of systems... this Regulation takes into account developments in international standards..."

Their implementation strategy included:

1. **Standards Gap Analysis**: Comprehensive assessment of current terminologies against required ISO IDMP standards
2. **Master Data Strategy**: Development of a unified approach to manage product and substance data
3. **Phased Implementation**: A three-tiered approach prioritising critical data domains
4. **Centralised Governance**: Creation of a cross-functional governance body to oversee standards adoption
5. **System Updates**: Modifications to core PV systems to support standardised terminologies
6. **Data Mapping**: Detailed mapping between legacy terms and new standardised terminology
7. **Change Management**: Robust communications and training plan for all affected stakeholders

The company successfully implemented the standards while minimising business disruption through careful planning and stakeholder engagement. Their phased approach allowed for course correction during implementation and focused resources on high-priority areas first.

Case Study 4: Building a Comprehensive Audit Program

A pharmaceutical company needed to strengthen its audit capabilities to meet the regulation's requirement that "Marketing authorisation holders shall perform regular audits of the quality system at risk-based intervals."

Their audit-focused approach included:

1. **Audit Program Design**: Development of a tiered audit framework with three levels of scrutiny based on risk
2. **Data Integrity Assessment**: Implementation of specialised data integrity audits focused on ALCOA+ principles
3. **Audit Tool Implementation**: Deployment of electronic audit management software with metrics dashboards
4. **Cross-Functional Auditor Training**: Creation of an auditor pool drawing from multiple departments
5. **Third-Party Audit Schedule**: Risk-based classification of vendors determining audit frequency and depth
6. **Audit Finding Categorisation**: Standardised approach to classify and prioritise remediation efforts
7. **Continuous Improvement Mechanism**: Process to incorporate learnings from each audit into program refinement

This approach shifted their focus from reactive to proactive quality management, allowing them to identify and address potential issues before they became regulatory findings.

Implementation Roadmap

A balanced implementation approach should:

1. **Assess Current State**: Conduct a holistic assessment covering systems, data governance, and audit programs
2. **Develop IT Quality Strategy**: Create an integrated approach addressing CSV, data integrity, and audit requirements
3. **Prioritise by Risk**: Focus on high-impact areas first, particularly those affecting patient safety
4. **Build Audit Program**: Establish or enhance risk-based audit capabilities, including third-party oversight
5. **Implement Data Governance Framework**: Deploy policies, procedures, and tools for robust data management
6. **Address CSV Requirements**: Conduct appropriate validation activities within the broader IT quality context
7. **Monitor Effectiveness**: Establish metrics to evaluate the performance of the overall IT quality program

Conclusion

The EU Pharmacovigilance Regulation amendment presents an opportunity to elevate IT quality management beyond traditional computer system validation. By implementing comprehensive approaches to audit, data governance, and data integrity alongside targeted CSV activities, organisations can build more resilient pharmacovigilance systems.

The most effective implementations will balance technical controls with strong governance processes, creating a foundation that supports both compliance and operational excellence. Whether leveraging experienced IT quality professionals or building capabilities internally, organisations should focus on developing an integrated approach that addresses the full spectrum of IT quality requirements.

With strategic planning and execution, these regulatory changes can drive meaningful improvements in pharmacovigilance systems, ultimately enhancing the industry's ability to protect patient safety through robust, reliable data management

---

This article provides a general analysis of the draft amendment to EU Regulation No 520/2012. Organisations should consult with their compliance teams and legal advisors for specific implementation guidance.