Guidance for IT Outsourced Cloud Computing and Data Integrity

Chris Wubbolt, QACV Consulting

Computer and Software Validation Conference
April 27, 2015
Objectives

- Provide an overview of how record integrity risks should be managed to comply with regulations.
- Review applicable regulatory requirements
- Discuss challenges when outsourcing to the cloud
- Ensuring data integrity
- Continuous monitoring for compliance
- Mitigating cloud computing risks
Record Integrity

What controls need to be considered?
Regulatory Requirements

21 CFR Part 11

Food and Drug Administration
August 20, 1997

Annex 11

European Commission
June 30, 2011
21 CFR Part 11
Electronic Records and Signatures

- Subpart A: General Provisions
- Subpart B: Electronic Records
  - Closed systems
  - Open systems
  - Signature manifestations
  - Signature/record linking
- Subpart C: Electronic Signatures
  - Electronic signature components and controls
  - Controls for identification codes/passwords
Electronic Recordkeeping Controls

- Validation
- Accurate and complete copies of records
- Records protection / retention
- Authorized system access
- Audit trails
- Operational System Checks

- Authority checks
- Device checks
- Personnel qualification
  - Develop
  - Maintain
  - Use
- Policies and Procedures
- System Documentation Controls
Annex 11
Computerised Systems

- Principle
- General
  - Risk management
  - Personnel
  - Suppliers and Service Providers
- Project Phase
  - Validation
Annex 11
Computerised Systems

Operational Phase

- Data
- Accuracy Checks
- Data Storage
- Printouts
- Audit Trails
- Change and Configuration Management
- Periodic Evaluation
- Security
- Incident Management
- Business Continuity
- Archiving
Software Applications

- ERP
- LIMS
- MES
- EDMS
- CDMS
- etc...
Cloud Computing - Historical Perspective

Software Applications
- ERP
- LIMS
- MES
- EDMS
- CDMS
- etc.....
Cloud Computing - Historical Perspective

Software Applications
- QMS

Saas Provider

Pharma A

Pharma B

Data Center
## Electronic Recordkeeping Controls

<table>
<thead>
<tr>
<th>Record Integrity</th>
<th>Record Availability</th>
<th>Record Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Record Integrity Compliance Program</td>
<td>- SOPs</td>
<td>- SOPs</td>
</tr>
<tr>
<td>- SOPs</td>
<td>- Change Control</td>
<td>- Change Control</td>
</tr>
<tr>
<td>- Validation</td>
<td>- Backup and Restore</td>
<td>- Backup and Restore</td>
</tr>
<tr>
<td>- Infrastructure Qualification</td>
<td>- Problem Reporting</td>
<td>- Business Continuity</td>
</tr>
<tr>
<td>- Security Program</td>
<td>- Business Continuity</td>
<td>- Business Continuity</td>
</tr>
<tr>
<td>- Training</td>
<td>- Disaster Recovery Plan</td>
<td>- Disaster Recovery Plan</td>
</tr>
<tr>
<td>- Change Control</td>
<td>- Record Retention Policy</td>
<td>- Record Retention Policy</td>
</tr>
<tr>
<td></td>
<td>- Archival</td>
<td></td>
</tr>
</tbody>
</table>
## Electronic Recordkeeping Controls

### Pharma Company
- Electronic Recordkeeping Compliance Program
- SOPs
- Validation
- Change Control
- Security Program
- Training
- Problem Reporting
- Business Continuity Plan
- Record Retention Policy

### SaaS Provider
- Electronic Recordkeeping Compliance Program
- SOPs
- Validation / SDLC
- Change Control
- Infrastructure Qualification
- Security Program
- Training
- Backup and Restore
- Problem Reporting
- Business Continuity
- Disaster Recovery Plan

---

4/28/2015
# Validation

## Pharma Company
- SOPs
- Validation Plan
- User Requirements Specification
- User Acceptance Testing (PQ)
- Traceability
- System Acceptance
- Validation Report

## SaaS Provider
- SOPs
- SDLC Methodology
- Functional Specification
- Configuration
- Installation (IQ)
- System Testing (Operational Qualification)
- System Release to Customer
- Traceability
Outsourced Cloud Computing

Validation

Clearly define responsibilities for shared validation and electronic recordkeeping controls.

The responsibilities can be defined within a Quality Agreement or Service Level Agreement.
Annex 11 – Risk Management

- Applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality.

- Decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment.
Documented evidence which provides a high degree of assurance that a system will consistently perform according to predetermined specifications and quality attributes.
Outsourced Cloud Computing

Conduct and document a risk assessment based on the risk of using the computerized system, including the outsourced computing environment to determine the extent of validation.
Suppliers and Service Providers

- Formal Agreements required to include clear statements of responsibilities

<table>
<thead>
<tr>
<th>Provide</th>
<th>Configure</th>
<th>Validate</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Integrate</td>
<td>Maintain</td>
<td>Retain</td>
</tr>
</tbody>
</table>

- IT departments should be considered analogous

- Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.
Outsourced Cloud Computing

Generate a Quality Agreement with your suppliers and service providers. Quality Agreements should include, minimally:

- Description of services provided
- Change Control
- Security
- Escalation processes
- Other quality requirements
Outsourced Cloud Computing

Other controls to consider

How will outsourced cloud computing partner be involved with:

- System administration
- Incident management
- Security
- Backup and restore
- Disaster recovery
- Personnel training
Questions
Contact Information

Chris Wubbolt
QACV Consulting, LLC

www.QACVConsulting.com

Telephone: 610-442-2250
E-mail: chris.wubbolt@QACVConsulting.com