Changing lives through learning

Qualification Unit

This unit forms part of a regulated qualification.

Unit Title: Data Integrity and Digital Systems

Unit Reference Number: R/652/4198

Level: Five (5)

Credit Value: 5

Minimum Guided Learning Hours: 35

Learning Outcome (The Learner will):	Assessment Criterion (The Learner can):
1. Understand data integrity principles and regulatory requirements for pharmaceutical digital systems	1.1 Evaluate data integrity principles and their application to pharmaceutical records
	1.2 Evaluate regulatory requirements and guidance relevant to pharmaceutical data integrity and electronic records
	1.3 Assess data-integrity risks associated with electronic records and pharmaceutical digital systems
	1.4 Evaluate the contribution of data integrity and digital systems to GMP compliance, product quality and patient safety
2. Be able to apply compliant practices to electronic records, audit trails and digital documentation	2.1 Interpret electronic audit trail records to identify potential data-integrity concerns
	2.2 Complete electronic pharmaceutical records in accordance with applicable documentation and data-integrity requirements
	2.3 Identify and correct electronic documentation errors using compliant amendment practices
	2.4 Evaluate the effectiveness of user access controls and authentication arrangements in maintaining data integrity
3. Understand the application, risks and validation requirements of digital systems used in pharmaceutical operations	3.1 Evaluate the functions and applications of digital systems used in pharmaceutical manufacturing and aseptic services

The intellectual property rights remain with Open Awards.

	3.2	Evaluate the contribution of digital systems to monitoring, controlling and documenting pharmaceutical processes
	3.3	Assess operational, data-integrity and cybersecurity risks associated with pharmaceutical digital systems
	3.4	Evaluate computerised system validation requirements and their contribution to maintaining a compliant state
4. Be able to evaluate data-integrity failures and develop appropriate quality-system responses	4.1	Analyse digital system and data-integrity evidence to identify deviations and assess their significance
	4.2	Apply structured investigation methods to identify potential causes of digital system or data-integrity failures
	4.3	Develop corrective and preventive recommendations to address digital system and data-integrity failures
	4.4	Evaluate digital system controls and develop recommendations for maintaining compliance and continuous improvement

Indicative Content	
LO1	1.1 must include ALCOA+ principles; attributable, legible, contemporaneous, original and accurate records; completeness, consistency, endurance and availability of data; application to electronic and paper-based records; data lifecycle and metadata. 1.2 must include relevant GMP requirements; EU GMP Annex 11; MHRA GxP Data Integrity Guidance; regulatory expectations for electronic records, data reliability and computerised systems. Other examples include FDA 21 CFR Part 11 where relevant to the operational context. 1.3 must include risks associated with data manipulation, loss, corruption, unauthorised access and incomplete recording; data lifecycle vulnerabilities; consequences of inadequate controls. Other examples include inappropriate data deletion, shared user accounts, missing audit trails and uncontrolled data transfers. 1.4 must include the role of reliable data in manufacturing and quality decisions; traceability and accountability; relationship between digital systems, GMP compliance and product quality; implications of data-integrity failures for regulatory compliance and patient safety.
LO2	2.1 must include the purpose and structure of audit trails; interpretation of recorded activities, user identities, timestamps and changes; identification of missing, unexplained or potentially unauthorised activities; implications for data reliability.

The intellectual property rights remain with Open Awards.

	2.2 must include accurate and contemporaneous electronic recording; use of appropriate user identification and authentication; completion and verification of required fields; adherence to relevant procedures and access permissions. Other examples include electronic batch records, digital logbooks, equipment interfaces and electronic monitoring records. 2.3 must include identification of inaccurate, incomplete or inconsistent electronic records; compliant correction procedures; preservation of original information and audit trail history; traceability, attribution and justification of amendments where required. 2.4 must include user access management; role-based permissions; authentication and electronic signatures; segregation of duties; risks associated with inappropriate access; effectiveness of controls in maintaining accountability and data reliability.
LO3	3.1 must include the functions and applications of laboratory information management systems (LIMS), manufacturing execution systems (MES), supervisory control and data acquisition (SCADA) systems and automated equipment interfaces; contribution to process monitoring, control, documentation and quality oversight. 3.2 must include collection and management of process data; automated monitoring and control; electronic documentation; traceability; availability of information for quality decisions; benefits and limitations of digital systems. Other examples include automated filling systems, equipment human-machine interfaces (HMIs), electronic batch records and digital environmental monitoring. 3.3 must include system failures, data loss, unauthorised access, cybersecurity vulnerabilities and system availability; potential implications for manufacturing continuity, data reliability, product quality and patient safety; relevant preventive and recovery controls. 3.4 must include principles of computerised system validation (CSV); risk-based validation; user requirements; qualification and testing; maintenance of the validated state; relevant Annex 11 expectations. Other examples include User Requirement Specifications (URS), Design Qualification (DQ), Installation Qualification (IQ), Operational Qualification (OQ), Performance Qualification (PQ), periodic review and change control.
LO4	4.1 must include examination of relevant electronic records, audit trails and system information; identification of data-integrity failures or deviations; assessment of potential impacts on data reliability, product quality, patient safety and regulatory compliance. 4.2 must include investigation of identified digital or data-integrity issues; review of available technical and quality evidence; assessment of system, procedural and human factors; identification of contributory factors and potential root causes. Other examples include inappropriate access permissions, system configuration weaknesses, equipment interface failures, inadequate training and procedural non-compliance. 4.3 must include selection of appropriate corrective and preventive measures; relationship between identified causes and proposed actions; consideration of system controls, procedures, training and data governance; justification of actions and measures for evaluating effectiveness.

The intellectual property rights remain with Open Awards.

	4.4 must include evaluation of existing or improved digital system controls; use of relevant quality and system performance evidence; identification of residual risks; change control considerations; recommendations for ongoing monitoring, risk reduction and continuous improvement.

The intellectual property rights remain with Open Awards.

Assessment Requirements

Assessment must demonstrate the application of specialist knowledge and skills relating to data integrity and digital systems within pharmaceutical manufacturing, aseptic services or pharmacy technical services environments.

Learners must demonstrate Level 5 analytical and evaluative capability, including the ability to interpret electronic records and audit trails, assess digital system risks, evaluate regulatory and validation requirements, investigate data-integrity concerns and develop justified recommendations.

LO2 and LO4 require evidence of applied skills. Learners must demonstrate compliant handling of electronic records, interpretation of audit trail information and application of investigation and quality improvement methods.

Assessment may use authentic workplace evidence or realistic technical scenarios supported by appropriate electronic records, audit trail extracts, system information and quality documentation.

Learners are not required to undertake software development, configure or administer live systems, independently validate computerised systems, approve CAPA or authorise changes to digital systems.

The qualification does not confer occupational competence or professional authorisation in its own right.

Evidence may include:

- Evaluations of data-integrity principles and regulatory requirements
- Data-integrity risk assessments
- Analysis of electronic audit trail records
- Completed electronic records or simulated electronic documentation
- Identification and correction of documentation errors
- Evaluations of user access and authentication controls
- Technical reviews of pharmaceutical digital systems
- Computerised system validation case studies
- Investigations into data-integrity deviations or system failures
- Root-cause analysis records
- CAPA recommendations and effectiveness evaluations
- Digital system improvement proposals
- Professional discussions supported by technical evidence

LO1 – Data integrity principles and regulatory requirements

Assessment should require learners to evaluate data-integrity principles and regulatory requirements within realistic pharmaceutical contexts.

Learners should consider the implications of data-integrity failures for product quality, traceability, regulatory compliance and patient safety.

Assessment should go beyond reproducing ALCOA+ definitions or describing individual regulatory documents.

The intellectual property rights remain with Open Awards.

LO2 – Electronic records and audit trails

Learners must interpret electronic audit trail evidence and demonstrate compliant completion and amendment of electronic documentation.

Assessment should include examples of audit trail entries or electronic records containing potential data-integrity concerns.

For AC 2.2 and 2.3, direct interaction with an appropriate electronic record system, training environment or realistic simulation should be used. Written explanations of documentation procedures alone are insufficient to demonstrate the required skills.

Where a simulated system is used, it must allow learners to demonstrate the relevant recording, amendment, attribution and traceability requirements. It need not reproduce the complete functionality of a commercial pharmaceutical system.

LO3 – Pharmaceutical digital systems

Learners should evaluate the application and risks of digital systems used within pharmaceutical operations.

Assessment should consider the contribution of systems to process control, documentation, monitoring and quality oversight.

For AC 3.4, learners should evaluate validation requirements for a relevant digital system, including appropriate qualification, testing and lifecycle considerations. They are not required to perform full computerised system validation.

LO4 – Data-integrity investigations and improvement

Learners must investigate a realistic digital system or data-integrity concern.

The assessment should provide sufficient evidence to allow consideration of potential system, procedural and human causes.

Learners should evaluate the significance of the issue, identify potential root causes and develop justified corrective or preventive recommendations.

For AC 4.4, learners should evaluate available evidence concerning the effectiveness of digital system controls. This may include post-implementation evidence supplied through a realistic case study where actual implementation is outside the learner's responsibilities.

An integrated assessment involving an electronic record review, identification of a data-integrity concern and subsequent investigation could provide evidence across LO2 and LO4.

The intellectual property rights remain with Open Awards.