Clinical Data Integration Compliance Checklist

Organization Name: _____

Date: _____

Reviewed By: _____

Checklist

	Requirement	Description	Compliant	Notes
1	Data Privacy Regulations	Ensure data integration adheres to GDPR, HIPAA, or local privacy laws.	â˜ Yes â˜ No	
2	Consent Management	Collect and manage patient consent for data sharing and integration.	â˜ Yes â˜ No	
3	Data Integrity	Validate data provenance and accuracy before integration.	â˜ Yes â˜ No	
4	Access Controls	Implement user authentication and role-based data access policies.	â˜ Yes â˜ No	
5	Audit Trails	Maintain logs of data integration activities and data access events.	â˜ Yes â˜ No	
6	Data Encryption	Apply encryption to data in transit and at rest.	â˜ Yes â˜ No	
7	Interoperability Standards	Use HL7, FHIR, or other recognized data exchange standards.	â˜ Yes â˜ No	
8	De-identification/Anonymization	Remove or mask patient identifiers where required.	â˜ Yes â˜ No	

| 9 | Data Retention & Deletion | Define periods for data storage and secure deletion protocols. | ☐ Yes ☐ No |
| 10 | Third-party Compliance | Verify compliance of vendors and integrated third-party systems. | ☐ Yes ☐ No |

Additional Comments

This checklist is a sample template and should be adapted to reflect project-specific regulatory requirements and organizational policies.