Advanced Data Privacy in Clinical Research (GDPR/HIPAA) Training Course

Professional Development Training Course Outline

Category	Biotechnology and Pharmaceutical Development	**Duration**	10 Days
Base Fee	$4,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The landscape of clinical research is fundamentally reliant on the ethical and legal handling of sensitive patient information. With the accelerating pace of digital transformation and globalized clinical trials, the risk of data breaches and non-compliance has never been higher. Advanced Data Privacy in Clinical Research (GDPR/HIPAA) Training Course provides essential, actionable knowledge for navigating the complex web of international data protection laws, specifically the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). It moves beyond basic awareness, focusing on strategic compliance, risk mitigation, and the operationalization of privacy-by-design principles within the entire research lifecycle.

Participants will master the critical distinctions and overlaps between these two landmark regulations, ensuring that cross-border data transfers are legal, secure, and maintain data subject rights. Key areas of focus include de-identification techniques, the role of the Data Protection Officer (DPO), managing data subject access requests (DSARs) in a research context, and implementing technical and organizational measures (TOMs) to achieve data sovereignty and accountability. This course is designed to empower research professionals to establish a trust-by-design culture, which is paramount for both ethical conduct and safeguarding the integrity of patient-centric research.

Programme Curriculum

Advanced Data Privacy in Clinical Research (GDPR/HIPAA) Training Course

Introduction

The landscape of clinical research is fundamentally reliant on the ethical and legal handling of sensitive patient information. With the accelerating pace of digital transformation and globalized clinical trials, the risk of data breaches and non-compliance has never been higher. Advanced Data Privacy in Clinical Research (GDPR/HIPAA) Training Course provides essential, actionable knowledge for navigating the complex web of international data protection laws, specifically the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). It moves beyond basic awareness, focusing on strategic compliance, risk mitigation, and the operationalization of privacy-by-design principles within the entire research lifecycle.

Participants will master the critical distinctions and overlaps between these two landmark regulations, ensuring that cross-border data transfers are legal, secure, and maintain data subject rights. Key areas of focus include de-identification techniques, the role of the Data Protection Officer (DPO), managing data subject access requests (DSARs) in a research context, and implementing technical and organizational measures (TOMs) to achieve data sovereignty and accountability. This course is designed to empower research professionals to establish a trust-by-design culture, which is paramount for both ethical conduct and safeguarding the integrity of patient-centric research.

Course Duration

10 days

Course Objectives

1. Master the intersection of GDPR and HIPAA mandates in multinational clinical trials.
2. Develop and implement Privacy-by-Design (PbD) and Security-by-Design frameworks for eConsent and eSource systems.
3. Execute compliant cross-border data transfers using Standard Contractual Clauses (SCCs) and Binding Corporate Rules
4. Conduct comprehensive Data Protection Impact Assessments (DPIAs) and Legitimate Interest Assessments (LIAs) for research protocols.
5. Apply advanced anonymization and pseudonymization techniques to maximize data utility while minimizing re-identification risk.
6. Formulate an effective data breach notification and incident response plan aligned with regulatory timelines.
7. Define and operationalize the roles of Controller and Processor under both GDPR and HIPAA Business Associate Agreements.
8. Implement Technical and Organizational Measures (TOMs), including Zero Trust Architecture and federated learning in data-sharing environments.
9. Effectively manage and respond to Data Subject Access Requests (DSARs) and the Right to Be Forgotten in the context of research data integrity.
10. Navigate the legal and ethical requirements for using de-identified and limited data sets (LDS) for secondary research and big data analytics.
11. Integrate ethical oversight and regulatory compliance for emerging technologies like AI/Machine Learning using Protected Health Information (PHI).
12. Establish robust data governance frameworks that ensure data quality, integrity, and accountability throughout the data lifecycle.
13. Prepare for and successfully navigate regulatory audits and inspections by demonstrating GDPR accountability and HIPAA compliance.

Target Audience

1. Clinical Trial Sponsors/CRO Leadership
2. Data Protection Officers (DPOs) and Privacy Program Managers in Pharma/Biotech
3. Clinical Research Associates (CRAs) and Clinical Data Managers
4. In-House Legal Counsel and Regulatory Affairs Professionals
5. Information Technology (IT) and Security Professionals
6. Institutional Review Board (IRB)/Ethics Committee Members
7. Principal Investigators and Site Research Coordinators
8. Bioinformatics and Health Data Scientists

Course Modules

Module 1: Foundational Principles and Regulatory Scope (GDPR/HIPAA)

- Defining Personal Data and Protected Health Information and the Overlap Rule.
- Understanding the legal bases for processing health data under GDPR Article 6 & 9.
- Identifying HIPAA Covered Entities and Business Associates in the research ecosystem.
- Case Study: Determining if a global CRO site operating in the EU is acting as a GDPR Controller or Processor for sponsor data.
- Comparative analysis.

Module 2: Privacy-by-Design and Security-by-Design

- Integrating Privacy Impact Assessments and DPIAs at the protocol design phase.
- Implementing data minimization and purpose limitation from trial start.
- Designing compliant eConsent forms that meet both GDPR transparency and HIPAA authorization requirements.
- Case Study: Conducting a DPIA for a Decentralized Clinical Trial involving patient wearables and remote monitoring.
- Establishing a Secure Software Development Lifecycle for clinical trial applications.

Module 3: Cross-Border Data Transfer Compliance

- Mechanisms for international data transfer.
- The impact of the Schrems II decision and the requirement for supplemental transfer risk assessments.
- Specific requirements for transferring PHI out of the US under HIPAA's Privacy Rule.
- Case Study: Drafting and implementing SCCs for transferring trial data from an EU site to a US-based sponsor's central database.
- Managing data localization and data residency requirements in complex jurisdictions.

Module 4: Advanced De-identification and Pseudonymization

- Distinction between HIPAA De-identification and GDPR Pseudonymisation vs. Anonymisation.
- Evaluating re-identification risk and the use of k-anonymity and l-diversity models.
- Implementing tokenization and data masking in clinical trial data warehouses.
- Case Study: Applying the Expert Determination standard to create a de-identified dataset for public deposition while maintaining research utility.
- Strategies for managing and securing the key-code linking pseudonyms to patient identifiers.

Module 5: Data Subject and Patient Rights Management

- Procedures for handling Data Subject Access Requests and the Right to Rectification within research timelines.

- Addressing the Right to Erasure and its limitations in GxP-regulated clinical data.
- Providing clear and accessible privacy notices that meet both GDPR and HIPAA requirements.
- Case Study: Developing a protocol to handle a participant's request for their trial data to be erased after the study concludes and data has been locked.
- Managing HIPAA's right to an accounting of disclosures for research use.

Module 6: Data Breach and Incident Response Planning

- Defining a reportable breach under GDPR and the HIPAA Breach Notification Rule.
- Developing a multi-jurisdictional incident response plan with pre-defined roles.
- Techniques for conducting a thorough risk assessment to determine the severity and necessity of notification.
- Case Study: Simulating a ransomware attack on an eCRF system and executing the breach notification plan to multiple DPAs and affected patients.
- The role of forensics and root cause analysis in breach documentation.

Module 7: Vendor Management and Third-Party Risk

- Negotiating and enforcing robust Business Associate Agreements under HIPAA with vendors.
- Drafting Data Processing Agreements under GDPR that specify sub-processor rules.
- Performing due diligence and continuous monitoring of cloud service providers for compliance.
- Case Study: Evaluating the compliance of a Software as a Service vendor providing remote patient monitoring tools across the US and EU.
- Contractual clauses for mandatory audit rights and immediate breach notification from vendors.

Module 8: Security Safeguards: Technical and Organizational Measures

- Implementing access controls and the principle of least privilege for clinical systems.
- Mandatory use of encryption for data in transit and at rest in accordance with both laws.
- Developing security policies and procedures as required by the HIPAA Security Rule
- Case Study: Designing a role-based access control (RBAC) matrix for a central clinical data management system to restrict access to PHI/PD.
- Requirements for audit logging, system monitoring, and periodic vulnerability testing.

Module 9: Data Governance and Lifecycle Management

- Establishing clear data retention policies and schedules compliant with GxP, GDPR, and HIPAA.
- Developing a structured archiving and secure destruction protocol for research records.
- Implementing data quality and integrity checks as a foundational security measure.
- Case Study: Defining the compliant process for destroying paper and electronic records after a 25-year post-study retention period.
- Creating a data inventory and record of processing activities as mandated by GDPR Article 30.

Module 10: Ethical Oversight and IRB/EC Interaction

- The IRB/Ethics Committee role in reviewing HIPAA Authorizations and GDPR consent forms.
- Distinction between Informed Consent and Authorization for use of PHI.
- Navigating the waiver or alteration of HIPAA Authorization for research purposes.
- Case Study: Presenting a new study protocol to a joint US/EU Ethics Review Board and justifying the secondary use of collected data.
- Ensuring transparency about data sharing and future research use in patient-facing documents.

Module 11: Special Categories of Data and Vulnerable Populations

- Specific GDPR Article 9 conditions for processing special categories of personal data
- Additional HIPAA requirements for research involving minors and individuals with diminished capacity.
- Addressing privacy concerns related to genomic data and the risk of familial re-identification.
- Case Study: Designing an ethical and compliant consent process for a pediatric clinical trial collecting genetic markers.
- Legal and ethical considerations for data collected via wearables and patient-generated health data

Module 12: Advanced Topics: AI, Big Data, and Federated Learning

- Privacy implications of using PHI for training AI/Machine Learning models in clinical research.
- Applying differential privacy and secure multi-party computation in collaborative research networks.
- GDPR Article 22 on automated decision-making and the right to human intervention in research outcomes.
- Case Study: Evaluating a federated learning model for a multi-site oncology study to ensure no raw patient data is shared.
- Addressing algorithmic bias and transparency when using AI for patient stratification or diagnostic support.

Module 13: Audits, Inspections, and Enforcement Actions

- Preparing for a Data Protection Authority inspection under GDPR.
- Best practices for demonstrating GDPR accountability through comprehensive documentation
- Responding to Office for Civil Rights audits and enforcement actions under HIPAA.
- Case Study: Responding to an official inquiry from a European DPA regarding the organization's Legal Basis for processing a specific trial's data.
- Implementing Corrective and Preventive Actions following an internal or external audit finding.

Module 14: Practical Tools: Templates and Checklists

- Reviewing and utilizing DPIA/PIA templates for standardized risk assessment.
- Checklists for BAA and DPA key clauses to ensure mandatory inclusion.
- Developing a concise GDPR Article 30 RoPA for clinical research activities.
- Case Study: Using a DSAR fulfillment checklist to ensure all legal requirements are met within the 30-day and 60-day deadlines.
- Walkthrough of a Security Risk Assessment tool to meet HIPAA requirements.

Module 15: Future Trends and Global Data Harmonization

- Emerging state-level US privacy laws and their impact on clinical research.
- The progression towards global data privacy standards and potential regulatory convergence.
- Implications of EU Health Data Space on data sharing for research.
- Case Study: Adapting a global SOP to account for a new national data sovereignty law requiring local data processing.
- Strategies for continuous regulatory intelligence and maintaining an agile compliance program.

Training Methodology

The course employs a **blended, highly interactive learning methodology** to ensure **actionable competence** and practical application.

1. Expert-Led Lectures.
2. Case Study Analysis.
3. Hands-On Workshops.
4. Interactive Q&A and Polls.
5. Role-Playing Simulations.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com