Taimei Technology

QUALITY AND INFORMATION SECURITY MANUAL

Biopharmaceutical Industry Practices

December 2023

Website
www.taimei.com

Contact us
BD@itaimei.com

DISCLAIMER

The content of this manual has been created by Taimei Technology's employees (referred to as the "Company"), and the Company legally owns all intellectual property rights associated with it.

This manual cannot be used as a basis for any other entity to comply with laws, regulations, or policies and is intended for reference purposes only.

For any matters not covered or omitted in this manual, please refer to the relevant national laws and regulations.

In the event of a conflict between the content of this manual and national laws and regulations, the national laws and regulations shall take precedence. The Company assumes no responsibility for any consequences resulting from the incorrect or illegal use of the content of this manual.

If the content, images, or other elements of this manual infringe upon the prior intellectual property rights of third parties or pose any risk of infringement, please contact us promptly for removal.

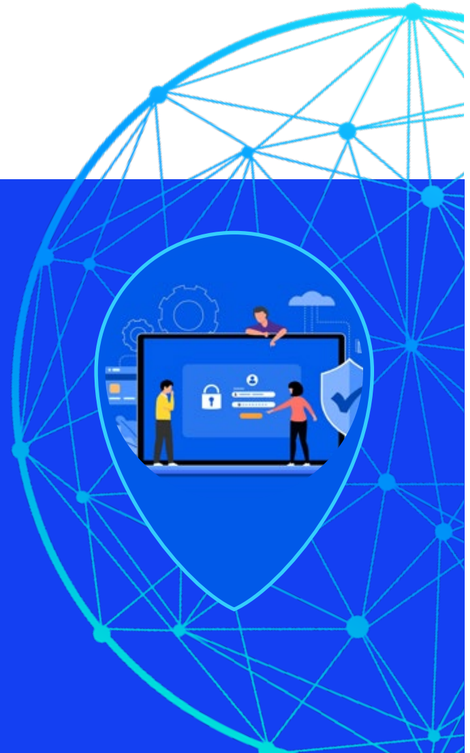
CONTENTS

CONTENTS

01

EVOLVING DATA SECURITY AND COMPLIANCE IN THE BIOPHARMACEUTICAL SECTOR

BACKGROUND INTRODUCTION



In recent years, data usage scenarios have become increasingly complex, with a growing global focus on data security. Prominent regulations such as the European Union's General Data Protection Regulation (GDPR) have been enacted, leading to significant fines ranging from hundreds of millions to billions of dollars.

The biopharmaceutical industry, being a critical sector related to public health, manages a substantial amount of personal and sensitive information. It necessitates a robust commitment to quality management and information security to effectively address both internal and external threats, prevent security incidents, safeguard patient interests, and uphold the economic interests and public reputation of biopharmaceutical companies.

Taking into consideration relevant laws, regulations, qualifications, and industry best practices, Taimei Technology has meticulously prepared this manual from an impartial standpoint. Our aspiration is that the insights into quality and information security presented in this manual can be shared across the industry, contributing to the enhancement of quality and information security systems within the sector.

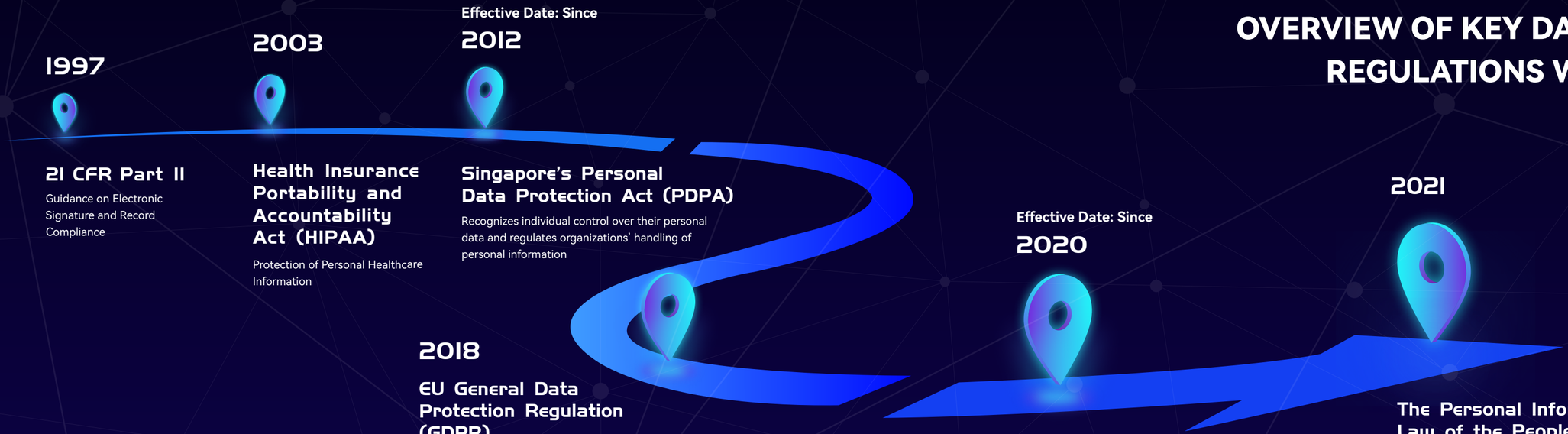
This document objectively showcases the endeavors and some notable accomplishments of Taimei Technology in the domains of quality and information security. We warmly invite our industry peers for discussions and knowledge sharing, aiming to collectively advance the progress of our field.

Evolving Data Security and Compliance in the biopharmaceutical Sector

STRATEGIES FOR UPHOLDING DATA INTEGRITY AND PRIVACY

02

OVERVIEW OF KEY DATA PRIVACY REGULATIONS WORLDWIDE



1997

21 CFR Part 11

Guidance on Electronic Signature and Record Compliance

2003

Health Insurance Portability and Accountability Act (HIPAA)

Protection of Personal Healthcare Information

Effective Date: Since 2012

Singapore's Personal Data Protection Act (PDPA)

Recognizes individual control over their personal data and regulates organizations' handling of personal information

2018

EU General Data Protection Regulation (GDPR)

Standardizes Privacy Protection Practices for EU Citizens

Effective Date: Since 2020

California Consumer Privacy Act (CCPA)

Regulates companies and individuals collecting and processing consumer personal information

2021

The Personal Information Protection Law of the People's Republic of China (PIPL)

Accelerating the Legalization Process of Personal Information Protection

The Personal Information Protection Law of the People's Republic of China

— A law specifically designed to safeguard personal information and protect individual rights

Biopharmaceutical Industry:

In numerous studies, it not only involves personal information but also more sensitive personal health and physiological data.

Key Highlights:

- **Explicit Consent:**

  In the biopharmaceutical industry, it is imperative to inform and obtain consent before handling personal information. Special authorization is mandatory for handling sensitive information.

- **Companies should establish:**

  A robust data security and lifecycle management system with rigorous control over data.

Strategies for Upholding Data Integrity and Privacy

The General Data Protection Regulation (GDPR)

— Legislation aimed at strengthening the privacy protection of EU citizens

Biopharmaceutical Industry:

Involving health data, GDPR mandates that any company processing information related to EU citizens must fulfill legal obligations and implement protective measures.

Key Highlights:

- **Personal Data Usage:**

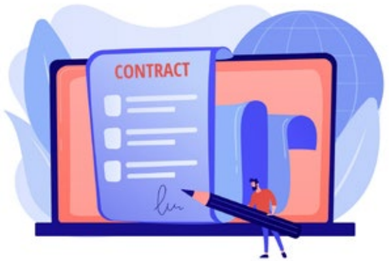
  Personal data, especially health data, should be used for specific purposes and within defined scopes, requiring individual consent.

- **Individual Rights:**

  Individuals have the right to exercise their rights, such as accessing information on the collection of their personal data as defined by the legislation.

Title 21 of the United States Code of Federal Regulations (21 CFR Part 11)

— Legislation issued and recognized by the FDA outlining terms for electronic records and electronic signatures



Biopharmaceutical Industry:

The most widely impactful legislation concerning electronic signatures and electronic records.

Key Highlights:

- Management of closed systems
- Audit trails
- Electronic signatures
- Signature forms

Health Insurance Portability and Accountability Act (HIPAA)

— Legislation issued by the U.S. government aimed at safeguarding individuals' healthcare information

Biopharmaceutical Industry:

Involves a significant amount of personal health information, and HIPAA constrains and regulates its use.

Key Highlights:

- **Privacy Protection Rules:**

  Privacy protection rules are established to specify principles governing the use and disclosure of Protected Health Information (PHI).

- **Collaborative Partner Contracts:**

  Collaborative partner contracts outline written guidelines for the use, protection, and disclosure of data.

03

INDUSTRY QUALIFICATIONS

01

ISO9001

Quality Management System Certification

- An internationally recognized, mature standard for quality management systems
- A strong proof that businesses can consistently provide high-quality products and services to their customers

02

ISO22301

Business Continuity Management System

- An internationally recognized management system standard for business continuity
- Aimed at maintaining the normal and stable operation of enterprise business in case of emergencies

Industry Qualifications

03

ISO27001

Information Security Management System Certification

- An internationally recognized standard for information security management systems
- Most biopharmaceutical companies worldwide have passed this certification

04

ISO27018

Public Cloud Personally Identifiable Information Management System Certification

- An internationally recognized standard for managing the protection of personally identifiable information in the cloud
- Meets the requirements of sponsors and regulators for the protection of personal information in biopharmaceutical companies

TRUSTe Certification:

— The preferred choice for most Chinese companies expanding internationally for privacy compliance certification

Focus of Certification:

· TRUSTe Certification:

Issued by TrustArc, a prominent US privacy certification organization.

· Privacy Framework:

— The privacy framework of the report is structured based on recognized legal standards (e.g., GDPR, HIPAA, etc.).

— This certification serves as compelling evidence of an enterprise's privacy compliance capabilities in the biopharmaceutical industry.

04

TAIMEI PRACTICES

ACCREDITATIONS & CERTIFICATIONS

ISO9001
Certification


DNV

MANAGEMENT SYSTEM CERTIFICATE

This is to certify that the management system of
Taimei Technology, Inc
Corporation Trust Center,1209 Orange Street in the City of Wilmington, County of New Castle,State of Delaware, Wilmington, USA
and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the Quality Management System standard:
GB/T 19001-2016 / ISO 9001:2015

This certificate is valid for the following scope:
Providing SaaS services for clinical trial and partner management

ISO22301
Certification


DNV

MANAGEMENT SYSTEM CERTIFICATE

This is to certify that the management system of
Taimei Technology, Inc
Corporation Trust Center,1209 Orange Street in the City of Wilmington, County of New Castle,State of Delaware, Wilmington, USA
and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the Business Continuity Management System Standard:
ISO 22301:2019

This certificate is valid for the following scope:
Providing SaaS services for clinical trial and partner management

ISO27001
Certification


DNV

MANAGEMENT SYSTEM CERTIFICATE

This is to certify that the management system of
Taimei Technology, Inc
Corporation Trust Center,1209 Orange Street in the City of Wilmington, County of New Castle,State of Delaware, Wilmington, USA
and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the Information Security Management System standard:
ISO/IEC 27001:2013

This certificate is valid for the following scope:
Providing SaaS services for clinical trial and partner management. This is in accordance with the latest Version of Statement of Applicability (Version 1.0)

ISO27018
Certification


DNV

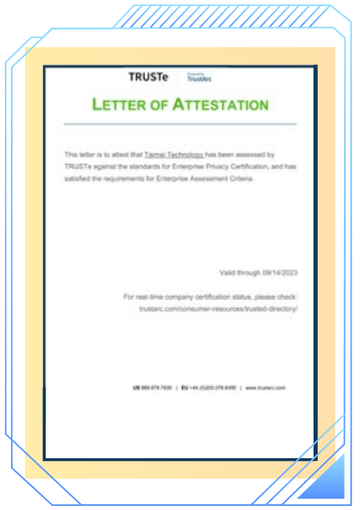
MANAGEMENT SYSTEM CERTIFICATE

This is to certify that the management system of
Taimei Technology, Inc
Corporation Trust Center, 1209 Orange Street in the City of Wilmington, County of New Castle, State of Delaware, Wilmington, USA
and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the Code of practice for information security controls:
ISO/IEC 27018:2019

This certificate is valid for the following Scope:
Providing Taimei Cloud SaaS Services for Clinical Trial and Partner Management, Use ISO27018:2019-Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds acting as PII Processor. This is in Accordance with the Latest Version of Statement of Applicability (Version 1.0). Associated with ISO27001 certificate 553917-2022-AIS-RGC-UKAS

TRUSTe
Certification


TRUSTe

LETTER OF ATTESTATION

This letter is to attest that Taimei Technology has been assessed by TRUSTe against the standards for Enterprise Privacy Certification, and has satisfied the requirements for Enterprise Assessment Criteria.

Valid through 09/14/2023

For real-time company certification status, please check: trustarc.com/consumer-resources/trusted-directory/

US 888.878.7830 | EU +44 (0)203 078 6495 | www.trustarc.com

Practices of 21 CFR Part 11

Closed System Management

Systems are released after verification according to recognized regulations, guidelines, and internal management procedures. Access protection for the system prevents any alterations to the system.

Electronic Signatures

Taimei Technology's products ensure the use of unique user IDs and passwords within the system. Each user ID can only appear once.

Signature Format

Electronic records (i.e., documents) can be configured by end-users for electronic signatures (approval). The signature's associated representation includes the printed name of the signer, the date and time of the signature execution, and the meaning of the signature. The electronic signature functionality enforces the consistent application of these components through logical design.

Audit Trail

Audit trails are retained for both operator interventions and automated execution sequences. This data record in the server center includes the file name, username, operation site/table/access, timestamps, operator actions, and potential new and old values.

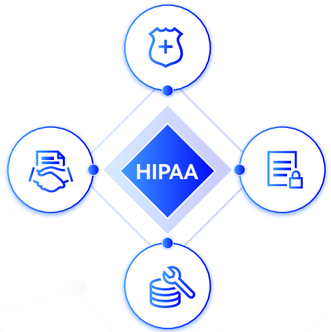
Practices of Health Insurance Portability and Accountability Act (HIPAA)

Identification and Protection of PHI (Protected Health Information)

PHI primarily comprises 19 types of information, including names, addresses, phone numbers, fax numbers, etc. It is essential to accurately identify PHI and implement various protection measures.

Partner Contracts

Define data usage conditions to ensure that data usage and disclosure strictly adhere to the contract's provisions. Protection requirements and details are explicitly stated.



Principles for Use and Disclosure

When using PHI, authorization from data subjects is obtained, and data is collected following the principle of minimalism. Privacy protection rules are adhered to when using and disclosing PHI.

Security Safeguard Standards

Establish security management policies and employ security technology controls to ensure the secure and reliable operation of systems.

Practices of General Data Protection Regulation (GDPR)

Compliance with Personal Data Processing Principles by Enterprises

Processing personal data in accordance with principles such as reasonable, legal, clear purpose, legitimate, and data minimization

Enterprise Data Protection Policy Formulation

Establish a comprehensive personal information security management system throughout the entire process and appoint the company's CTO as the DPO

Company Response to Data Subject Rights

Taimei Technology informs data subjects of their right to rectification and other relevant rights, providing methods for data subjects to exercise these rights

Adoption of Data System Security Measures

Implementing appropriate security measures to ensure the confidentiality, integrity, and availability of systems and services, taking measures to defend against data loss, tampering, and other threats to personal data

Recording Data Processing Activities

Taimei Technology maintains records of data processing activities for which it is responsible

Practices of Personal Information Protection Law of the People's Republic of China

Reasonable Necessity in Personal Data Processing

- Regular personal data protection reviews
- Consistency of processing principles and privacy text

Security of Personal Information Processing

- The entire lifecycle of personal information
- Information security solutions and frameworks

Individual Rights Response Mechanism

- Explained in the privacy policy or informed consent form
- Timely response within fifteen days in the background

Personal Information Security Audit

- Regularly review business operations to ensure compliance
- Form a compliant closed loop throughout the entire lifecycle of personal information

Personal Information Processor Security Strategy

- Achieved ISO 27001 Information Security Management System Certification
- Implement classified and labeled management for personal information

Changes to Personal Information Processing Principles

- Update privacy policy or informed consent document
- Notify users again and obtain consent