

ICS 35.240
CCS L 60



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 46284-2025

**Artificial intelligence - Technical specifications of federated
learning**

人工智能 联邦学习技术规范

Issued on: October 5, 2025

Implemented on: October 5, 2025

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

1.Scope	1
2 Normative References	1
3.Terms and Definitions	1
4.Abbreviations	2
5.Overview of Federated Learning Systems	2
5.1 Federated Learning System Architecture	2
5.2 Participants in Federated Learning	3
5.3 Federated Learning Task Process	5
6.1 Basic Technology Module	7
6.2 Calculation Module	8
6.3 Management Module	8
7.Federated Learning System Performance Requirements	10
7.1 Federal Data Probing	10
7.2 Federated Modeling	10
7.3 Federalized Reasoning	11
7.4 Federal Data Quality and Incentive Mechanisms	11
8.Functional Testing Methods for Federated Learning Systems	11
8.1 Basic Technology Module	11
8.2 Calculation Module	12
8.3 Management Module	13
9.Performance Testing Methods for Federated Learning Systems	15
9.1 Federal Data Probing	15
9.2 Federated Modeling	16
9.3 Federalized Reasoning	16
16 Reference	18

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1.Structure and Drafting Rules of Standardization Documents". Drafting. Please note that some content in this document may involve patents. The issuing organization of this

document assumes no responsibility for identifying patents. This document was proposed and is under the jurisdiction of the National Information Technology Standardization Technical Committee (SAC/TC28). This document was drafted by: China Electronics Technology Standardization Institute, Shenzhen Qianhai WeBank Co., Ltd., and China Mobile Communications Corporation. Research Institute of China Electronics Technology Group Corporation Limited, China Mobile Communications Group Co., Ltd., Industrial and Commercial Bank of China Limited, China Electronics Technology Big Data Research Institute Co., Ltd. Company, Shenzhen Insight Wisdom Technology Co., Ltd., Inspur Software Technology Co., Ltd., Inspur Software Group Co., Ltd., Shandong University, Harbin Shenzhen Institute of Technology, Inspur Electronic Information Industry Co., Ltd., China Mobile (Suzhou) Software Technology Co., Ltd., AsiaInfo Technologies (China) Co., Ltd. Limited Company, Beijing Shudu Technology Co., Ltd., Institute of Computing Technology, Chinese Academy of Sciences, OPPO Guangdong Mobile Communications Co., Ltd., Shanghai Artificial Intelligence Industry Association, Shanghai Computer Software Technology Development Center, Institute of Automation, Chinese Academy of Sciences, China Telecom Research Institute, China Southern Power Grid Data Platform and Security (Guangdong) Co., Ltd., Shanghai Lingshu Zhonghe Information Technology Co., Ltd., and Mashang Consumer Finance Co., Ltd. Limited Liability Company, Bank of Communications Co., Ltd., Hangzhou High-tech Zone (Binjiang) Blockchain and Data Security Research Institute, Hangzhou QuChain Technology Co., Ltd. Beijing Haohan Depth Information Technology Co., Ltd. This document was drafted by: Fan Kefeng, Fan Lixin, Ma Shanshan, Qian Wenjun, Jia Yunfei, Xia Zhiyuan, Guan Guilin, Wang Wanwan, Lin Yiwei, and Meng Jian. Wu Jianlong, Nie Liqiang, Di Helang, Wang Xiaobin, Jing Qin, Jin Yinyu, Wang Yuwei, Fu Yanyan, Rao Xue, Chen Mingang, He Saike, Wu Zuping, Yang Guang Lan Chunjia, Deng Weihong, Wang Guangzhong, Du Jingyi, Zhang Qing, Liu Shaokai. Artificial Intelligence Federated Learning Technical Specifications

1 Scope

GB/T 46284-2025 is the Chinese national standard covering training a model without moving the data - the horizontal and vertical arrangements, the aggregation of updates rather than of records, the encryption and the differential privacy that stop the updates leaking what they were computed from, and the contribution accounting between the parties. First edition, and it is the technical basis for the data-sharing arrangements Chinese privacy law otherwise makes difficult. Already in force. Issued on 5 October 2025, it has been in force since 5 October 2025.

This document establishes the architecture, participants, and workflow of the federated learning system, and specifies its functional requirements and performance. The requirements describe the corresponding testing methods. This document applies to the design, development, testing, use, and maintenance of federated learning systems, and to conducting horizontal comparisons of federated learning application systems. Selection.

Note. This document only covers the system functionalities and performance requirements for implementing and supporting federated learning methods; it does not provide details on general-purpose computer hardware and software or communication equipment itself. Detailed regulations.

2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included. For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies. This document.

GB/T 41867 Terminology for Information Technology and Artificial Intelligence

3 Terms and Definitions

The terms and definitions defined in GB/T 41867 and the following terms and definitions apply to this document.

3.1 Federated learning Multiple participants interact in a manner that protects privacy, while ensuring that their original data does not leave the trusted domain defined by the data provider. Methods for collaboratively completing artificial intelligence and machine learning tasks by using inter-data.

3.2 A comprehensive computer and communication system for implementing federated learning methods.

Note. This system includes not only various computer hardware and software (such as algorithms, CPUs, GPUs, etc.) for executing federated learning algorithms, but also supports remote communication between nodes. The communication protocols and equipment used for data transmission (e.g., network devices and data transmission protocols). This system ensures that each participant can protect the original data locally. Under the premise of privacy, machine learning tasks can be completed collaboratively by exchanging intermediate model updates (such as gradients or parameters).

3.3 In federated learning methods that divide data into samples, each participant's dataset has the same feature space but different sample spaces.

3.4 In a feature-based federated learning approach, each participant's dataset has the same sample space but different feature spaces.