Journal of Electronic Research and Application, 2026, Volume 10, Issue 3
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Practices and Insights of Scientific Data Security Grading Management Based on the Entire Life Cycle

Yu Zhai, Yong Song

Xinjiang Academy of Science and Technology for Development, Urumqi 830011, China

Abstract: In the era of big data, scientific data has become a strategic resource for national scientific and technological innovation and economic and social development, and the importance of its security management has become increasingly prominent. Based on the theory of the entire life cycle management of scientific data, this paper deeply discusses the core connotation of data security grading management, and systematically analyzes the prominent problems existing in the current scientific data security management in terms of system connection, process coverage, technology adaptation, and rights protection. On this basis, the paper constructs a practical path of scientific data security grading management covering six stages: data planning, collection, storage, use, sharing, and destruction, and puts forward targeted implementation strategies. Research shows that scientific data security grading management based on the entire life cycle is not only a technical issue but also a systematic project involving system design, organizational collaboration, and cultural cultivation. It has important theoretical value and practical enlightenment for improving data governance capabilities and promoting the orderly opening and sharing of scientific data.

Keywords: Scientific data; Entire life cycle; Data grading; Security management; Data governance

Online publication: April 22, 2026

1. Introduction

As scientific research enters the era of the fourth paradigm, scientific data has shown an explosive growth trend, with an unprecedented scale, variety, and flow speed. Scientific data is not only the basic output of scientific research activities but also the core element supporting major scientific discoveries and driving economic and social innovation [1]. Scientific data security grading management based on the entire life cycle emphasizes embedding security controls into the complete process of data from generation to destruction, and adopting differentiated protection measures according to the differences in data sensitivity and importance. This concept provides a new idea for solving the dilemma of "difficulty in sharing and protecting" scientific data [2]. This paper aims to sort out the core connotation of scientific data security grading management based on the entire life cycle, analyze the problems existing in current practices, and explore a systematic practical path, so as to provide useful reference for improving China's scientific data security management system.

2. Core connotation of scientific data security grading management based on the entire life cycle

Scientific data security grading management based on the entire life cycle is essentially a data governance model that combines process control theory and risk management methods. Its core connotation can be understood from three dimensions.

2.1. Entire life cycle

From the perspective of the "entire life cycle", scientific data is not a static entity but undergoes a dynamic process of generation, processing, analysis, storage, sharing, reuse, and ultimately destruction. Each stage faces different security threats and corresponds to different management objectives and responsible subjects [3]. For example, in the data collection stage, the main risk points lie in the credibility of collection equipment and the integrity of the collection process; in the data sharing stage, it is necessary to focus on the rigor of access control and the effectiveness of data desensitization. Therefore, security management cannot only focus on a single link but should build a closed-loop control system covering the entire life cycle of data.

2.2. Grading management

"Grading management" is the essence of this model. There are significant differences in the value density and security sensitivity of scientific data. Basic and public welfare observation data and scientific research data involving national secrets, trade secrets, or personal privacy cannot be managed with the same standards. Grading management requires the establishment of scientific and reasonable grading standards. According to factors such as data content attributes, source channels, aggregation effects, and open risks, data is divided into different security levels, and corresponding technical protection measures and management processes are configured accordingly.

2.3. Dynamic adjustment and collaborative linkage

This model emphasizes "dynamic adjustment" and "collaborative linkage". The life cycle of data does not advance linearly but may cycle between different stages; at the same time, the security level of data may change with the evolution of application scenarios, the degree of data aggregation, and the external environment. Therefore, grading management must be dynamic and iterable, and require multi-party collaboration among data managers, data producers, data users, and even regulatory authorities to form a joint force for security governance. In a word, the core of this model is to embed the concept of security into every link of data flow, and achieve a dynamic balance between security and sharing through refined grading strategies [4–6].

3. Problems existing in scientific data security management

3.1. Ambiguous grading standards and poor system connection

China's existing data security management mainly faces the problems of ambiguous classification and fragmented management systems. The Data Security Law and the Measures for the Management of Scientific Data only make principled provisions on data classification, but lack detailed implementation rules for data management targeting specific types such as scientific data. There is a lack of clear, specific, and operable grading standard systems. Data characteristics vary greatly in different fields. For example, experimental data in the field of high-energy physics and genetic data in the field of biomedicine have completely different requirements in terms of sensitivity and security. Existing norms often cannot meet the requirements of various disciplines, bringing troubles to data

managers. Secondly, the management of scientific data lacks good connection with the protection of national secrets, trade secrets, and personal privacy in other laws and regulations, and there are institutional blind spots or conflicts to a certain extent, resulting in high costs for carrying out data security protection and applications [7].

3.2. Incomplete coverage of the life cycle and shortcomings in key links

In practice, most data security subjects focus on the storage link, only paying attention to the physical and network boundary protection of data centers, while ignoring potential risks in other links of the entire data life cycle, especially the original data generated by collection links such as field stations and experimental instruments. The security of communication links and terminal authentication are often ignored. In the process of data utilization and sharing, there is a lack of fine-grained authorization mechanisms and dynamic behavior auditing, resulting in risks such as unauthorized access, illegal copying, and even secondary transmission by employees; there is generally a management blind spot in the data destruction link. Even if there are explicit regulations from hard disk destruction to the deletion of unused files, the actual execution process cannot be effectively monitored, which may lead to the leakage of sensitive information and bring security risks.

3.3. Disconnection between technology and business and insufficient grading protection capabilities

Although technology is an important means for grading control, it also faces the dilemma of "two skins" between technology and business in practice: on the one hand, most existing security technology facilities adopt a general design model and cannot accurately match the network traffic characteristics and user behavior of specific scientific research units; for example, excessive information confidentiality will lead to inefficient processing of a large amount of scientific research information, which may reduce the efficiency of scientific and technological research and development [8]. In addition, many institutions have not well integrated the level system management in the process of using security technology. For example, after data is classified, there is still no good method and technical support to automatically trigger relevant encryption, desensitization, and access control strategies. The intelligent and automated label recognition technology and strategy implementation capabilities are still lacking, so it is impossible to achieve refined grading control, which is often manifested as extensive "one-size-fits-all" management.

3.4. Complex interest relationships and difficulty in balancing security and sharing

Scientific information often involves many stakeholders: data producers, data processors, fund providers, data owners, and potential re-users, which makes graded and classified governance face complex challenges. On the one hand, out of consideration for protecting their own research results and intellectual property rights, individual scientists or research teams will adopt overly conservative data control strategies. For instance, basic data that should be open is deliberately closed, affecting communication and authentication among the scientific community. Moreover, there is a lack of specific right definition and benefit-sharing system design. Management institutions tend to adopt the strictest security protection measures to avoid liability risks, resulting in a large amount of valuable scientific data being idle and failing to play its due value function. Therefore, how to break these barriers and achieve legal and compliant scientific data sharing on the premise of ensuring the security of important data is the primary problem to be solved in graded and classified management [9].

4. Practical path of scientific data security grading management based on the entire life cycle

4.1. Planning stage: Establish grading principles and institutional systems

Before carrying out the security level control of scientific data, top-level design and planning should be done well, that is, a joint working group composed of data managers, researchers, information security departments, and legal departments should jointly formulate management measures for the security guarantee level of scientific data. This measure mainly clarifies the classification standards and scope. In practice, classification should be based on data secrecy level, completeness, and purpose. On this basis, a data classification directory within the unit or field should be formulated, and clear provisions should be made on the data meaning, identification method, protection criteria, and applicable conditions represented by each category [10]. In addition, the post responsibilities in each link should be clarified, the responsibility of classified management should be specifically assigned to the corresponding departments and individuals, and a dynamic communication, coordination, and supervision mechanism should be established to ensure that the classified management work has rules to follow and evidence to rely on.

4.2. Collection and processing stage: Implement source grading and label embedding

The first stage is the collection process and data analysis process. In this process, the first step of classified management is carried out, that is, establishing a dynamically generated classified data model. During the research project approval and data collection, the project leader should predict the data to be produced according to the existing classification system. For data containing important sensitive information, such as human genome data and the operation status of important facilities, a special security assessment should be conducted and a collection plan formulated before collection; during the data collection process, it is necessary to ensure the security of the collection terminal and adopt initial encryption means. A restricted environment should also be established in the process of data cleaning, labeling, re-identification, fusion, etc. In this link, data security labels should be taken as an important part of metadata to ensure that the data security level exists throughout the data circulation, laying a foundation for the automated and refined management of subsequent links. When de-identified information can reduce the sensitivity level, a strict review mechanism should be established to conduct a secondary verification of its security [11–13].

4.3. Storage and use stage: Implement differentiated protection and dynamic access control

In the entire life cycle of data, the storage link and use link are the two most important links with the most interactions, so the security management requirements of these two links are also the highest. In terms of the storage link, different levels of physical security management and logical security protection measures should be implemented according to the degree of data importance; for important data, encrypted storage, off-site multiple backups, and special person custody should be adopted; for critical data, access domain control should be carried out and regular backups should be made [14]. For general data, only basic security requirements need to be met. In terms of data application, an attribute-based dynamic access control mechanism should be established, that is, not only based on static identity permissions but also real-time judgment on the legality of access requests according to factors such as user identity, data level, application scenario, and application purpose. For example, for high-level data, computing services should be provided in a secure sandbox to “make data visible but unavailable”. At the same time, strengthen the control of the entire life cycle of data use, especially the real-time monitoring and

abnormal behavior alarm of high-risk operations (search, download, copy) involving high-level data, thus forming effective influence and traceability.

4.4. Sharing and destruction stage: Standardize circulation procedures and closed-loop termination management

The sharing and destruction links are the most dangerous links in the entire data life cycle. During this period, the "minimum necessary principle" should be followed to determine the specific content of data sharing and the security level of sharing objects. Low-security-level data can be released on public databases; medium-security-level data can be shared by signing agreements, clarifying the scope of use, objects of use, duration of use, and violation penalties; sensitive data is usually only allowed to be accessed by certain personnel in a restricted manner in an internal environment, and the leakage of original data is strictly prohibited. During the sharing process, a complete traceable approval flow and flow record should be available. Data destruction is the last link in the entire life cycle and is often ignored [15]. When data exceeds the validity period, completes the established task, or in accordance with legal and regulatory requirements, the data should be destroyed in accordance with procedures. Destruction methods include logical deletion, clearing hard disk data, destroying storage media, etc. According to the data level, it should be carried out in accordance with the two-person system, full-process monitoring, and final confirmation. For external storage media or discarded media, a confidentiality agreement must be signed before supervising the destruction process to avoid information leakage risks caused by improper disposal of discarded media. Now, scientific data is in a complete chain from birth to death, with hierarchical management throughout.

5. Conclusion

Scientific data security grading management based on the entire life cycle is a profound reform of the traditional static and local security thinking. It requires us to view scientific data from a developmental and interconnected perspective and deeply embed security capabilities into the blood of data flow. The scientific data security grading management model based on the entire life cycle is not only a pile of technical tools but also a comprehensive governance framework covering system design, process optimization, organizational collaboration, and cultural cultivation. Its successful practice relies on clear grading standards, full-chain control measures, high integration of technology and business, and prudent balance of multiple interests. At present, China is thoroughly implementing the innovation-driven development strategy and the big data strategy, and the status of scientific data as a national basic strategic resource has become increasingly prominent. Building a scientific, efficient, and entire life cycle security grading management system that meets the requirements of the data element era is of far-reaching significance for safeguarding national security, stimulating innovation vitality, and improving governance efficiency.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Ren J, Xie Y, Wang T, et al., 2025, Construction of Source Governance and Security Protection System for

Government Personal Information from the Perspective of Data Entire Life Cycle. Computer Knowledge and Technology, 21(36): 68–70.

[2] Xiao J, 2025, Research on the Integrated Management of Electronic Documents Throughout the Life Cycle Under the Background of Government Big Data. Shanxi Archives, 2025(12): 155–157.

[3] Li X, Li K, 2026, Specific Scenarios, Key Risks and System Construction of AI Data Cross-Border Security Supervision from the Perspective of the Entire Life Cycle. Hebei Law Science, 44(2): 101–122.

[4] Xuan W, 2025, "Roadmap" for the Open Sharing of Scientific Data Under the Data Intelligence Paradigm: Recommendation of Open Sharing of Scientific Data: From Ownership Definition to Management System Construction. Information Studies: Theory & Application, 48(11): 211.

[5] Fan B, Duan J, Zhang Y, et al., 2025, Research on Data Security Classification and Grading Management Based on Artificial Intelligence. Network Security & Informatization, 2025(11): 20–21.

[6] Huang S, Chen G, Jin M, et al., 2025, Classification and Grading Management and Security Protection of Data Assets in the Era of Big Data. Digital Communication World, 2025(9): 142–144.

[7] Hao Y, Li D, Han L, et al., 2024, Research and Preliminary Practice of Full-Cycle Data Security Management for Data Middle Platform: A Case Study of National Natural Science Foundation Data Management. Science Foundation in China, 38(4): 696–702.

[8] Gao W, Xu B, Li Z, et al., 2024, Application of Visual Malware Analysis Technology in Data Science in the Digital Archive Security Management System. Network Security and Data Governance, 43(5): 18–26.

[9] Zhang G, Wang J, Pan Y, et al., 2024, Research on Security Management Strategies and Typical Practices of Scientific Data Sharing Platforms at Home and Abroad. Forum on Science and Technology in China, 2024(4): 179–188.

[10] Huang Y, 2023, Research Report on the Data Application Security Mechanism of Customs Based on Grading Management. Dalian Customs, Liaoning Province, November 22, 2023.

[11] Chang Z, Ye X, Liu W, et al., 2023, Construction of Process-Oriented Management and Risk Control System Model for Scientific Data Security Platform. Information Research, 2023(11): 66–73.

[12] Wu D, Zhao X, Ma D, et al., 2023, Data Security Compliance Management Solution for the National Statistical System, Proceedings of the 2023 Cybersecurity Excellent Innovation Achievements Competition, 4.

[13] Zou C, Ma H, Wang J, 2023, Performance Analysis Framework and Configuration Analysis of Public Data Security Management. Library and Information Service, 67(13): 70–77.

[14] Liu X, Sun M, 2023, Practices and Insights of Scientific Data Security Grading Management from the Perspective of the Life Cycle. Information Studies: Theory & Application, 46(3): 68–74.

[15] Huang Y, 2022, Analysis of Scientific Data Security Management Strategies in American Libraries in the Digital Economy Era. Library and Information Guide, 7(9): 15–19.