Guidelines for safety management of medical Information using **Acronis** Cyber Protect Cloud

This document provides an overview of the security management measures implemented by Acronis as a part of the information disclosure requirement under "The Safety Management Guideline for Information Systems and Service Providers Handling Medical Information," v 1.1 reviewed in August 2023, required by the Ministry of Economy, Trade, and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC). Acronis' controls described in this document are certified by the third-party audit compliance programs ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 and ISO 9001; other detailed information can be acquired via SOC-2 Type II report.

Since the "information flow" required by the "The Safety Management Guideline for Information Systems and Service Providers Handling Medical Information" differs for each Acronis user, it is difficult to present the response for each situation. Therefore, Acronis drafted this document according to the "Attachment 2 List of countermeasure items in preintegration guidelines and correspondence table of medical information safety management guidelines version 6.0." In addition to the numbering used in Attachment 2 and the corresponding "content of the requirement," the table below includes details on how Acronis complies with each requirement, along with a map linking the relevant ISO controls.

[1] https://www.soumu.go.jp/main_content/000891033.pdf
[1] https://www.soumu.go.jp/main_content/000891035.pdf

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
1. Human and Organizational Measures				
1.1. Establishment of policies and procedures	❶ Establishment of access management policies	❶-1	Create access management policies which define access restrictions, records, monitoring for medical information systems. Make them available for submission upon request from medical institutions.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Access Control” (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis’ ISO/IEC 27001 and SOC 2, Type II report. Acronis as a company differentiates between two types of data: • Data necessary for providing the services (e.g., product usage) and Acronis’ service management. This is the data which Acronis collects and processes as a data controller for providing our services. Such data may include account names, email and other contact details, billing details and some information automatically collected via the service, which may be personal. For more details, please check the Acronis Privacy Statement: https://www.acronis.com/company/privacy/. • Customers’ content data. This is the data which Acronis may process as a data processor (subprocessor) when you use our services. The information is provided by customers while utilizing the specific products — e.g., backup archives, files, virtual machines, etc. In terms of this type of data, Acronis does not control the categories and the content of the information which customers are storing with us. Acronis keeps strict segregation of duties and grants privileged access on role base. Acronis’ employees do not have access to customers’ content data. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.
		❶-2	The Access control procedures shall include the following contents: • Registration, change, disposal application, and approval, as well as periodic verification processes for access rights and account management. • Storage and collection of records for authentication and access, etc. • Periodic review of records for authentication and access, etc. • Regular review of the operational status of access control.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Access Control” (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • “Documented Operating Procedures” (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). Information security oversight and management controls, including logical access controls, are reviewed and verified by a third-party auditor for Acronis’ ISO/IEC 27001 and SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management according to their own needs.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	❷ Measures for connecting to external networks when using corporate mobile device	❷-1	Include specific measures into the operational management policies to ensure that when connecting corporate mobile devices to external networks, connection conditions and security measures are implemented (such as: specific measures to prevent leakage or tampering of stored information, measures against malicious software, encryption, and implementation of firewalls).	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • "Documented Operating Procedures" (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). • "Networks security" (ISO27K1:2013 A.13.1; ISO27K1:2022 A.8.20, A.8.22). • "Data leakage prevention" (27K1:2022 8.12). Information security oversight and management controls, including logical access controls, are reviewed and verified by a third-party auditor for Acronis' ISO/IEC 27001 and SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including development of operational procedures and guidelines.
	❸ Disposal procedures for information	❸-1	Establish disposal procedures for CD-Rs, etc.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Removal of assets" (27K1:2013 A.11.2.5; 27K1:2022 A.7.10). • "Equipment maintenance" (27K1:2013 A.11.2.4; 27K1:2022 A.13). • "Documented Operating Procedures" (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). Information security oversight and management controls, including logical access controls, are reviewed and verified by a third-party auditor for Acronis' ISO/IEC 27001 and SOC 2, Type II report. Acronis hard drives incorporate technologies such as full-disk encryption (FDE) and drive locking mechanisms to secure data at rest. Acronis, within data center colocation, uses local qualified third parties to ensure physical disposal of drives.
		❸-2	Establish disposal procedures for hard disks, etc.	
		❸-3	In the disposal procedures, include measures for irreversible destruction, deletion, etc., to ensure that the original data cannot be recovered.	
		❸-4	When reusing hard disks or other devices within medical information systems or similar systems, ensure that data is erased using a reliable method, such as multiple data overwrite processes, to securely erase the original data. Confirm that the information has been erased before reuse.	
		❸-5	If passwords, such as BIOS passwords for servers or hard disk passwords for hardware, are set, ensure they are erased.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❸-6	When connecting a hard disk to a device, regardless of whether it is for reuse or not, verify with a validation device that no unauthorized programs or data are recorded.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Protection against malware" (27K1:2013 A.12.2; 27K1:2022 8.7). • "Management of technical vulnerabilities" (27K1:2013 A.12.6.1, A.18.2.3; 27K1:2022 A.8.8). Acronis implements a comprehensive vulnerability management program that proactively identifies security threats through a blend of market-available and custom-developed in-house tools, alongside rigorous automated and manual penetration testing, quality assurance measures, software security assessments, and external audits. The responsibility for monitoring and addressing vulnerabilities lies with the Acronis cybersecurity team, which meticulously identifies and tracks these issues, ensuring regular follow up until remediation is confirmed. Furthermore, Acronis cultivates strong connections with independent security researchers running a bug bounty program. Controls relating to vulnerability management are also reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. More information on Acronis' cybersecurity posture can be found at https://www.acronis.com/trust-center/
		❸-7	For the disposal of hard disks, implement measures such as multiple data overwrite to ensure that reuse and data retrieval are impossible. Also, apply measures such as data erasure by strong magnetic fields and physical destruction (melting by high temperatures, shredding, etc.). Maintain records summarizing the implemented measures for the respective device (format of the equipment, identification number, responsible personnel, date and time of implementation, details of the procedure, etc.). Ensure that these records can be promptly submitted upon request from medical institutions, etc.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Removal of assets" (27K1:2013 A.11.2.5; 27K1:2022 A.7.10) • "Equipment maintenance" (27K1:2013 A.11.2.4; 27K1:2022 A.13). • "Documented Operating Procedures" (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). Information security oversight and management controls, including media security are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis hard drives incorporate technologies such as full-disk encryption (FDE) and drive locking mechanisms to secure data at rest. Acronis uses a software-defined storage solution, which utilizes a proprietary erasure-coding algorithm, and which securely removes customer data. In the case Acronis Cyber Infrastructure drives and equipment are broken, switched out for repair or decommissioned, Acronis takes measures to erase data from a disk and remove residual data from the internal memory of the equipment, according to NIST SP 800-88rev1. In the event that it is not possible to erase (delete) such information, equipment is physically destroyed in such a way that it's impossible to read (restore) such data. Acronis, within data center colocation, uses local qualified third parties to ensure physical disposal of drives. Customers are solely responsible for evaluating and maintaining their own legal and compliance obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with its customers, who have such obligation under applicable data protection regimes.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		③-8	It is recommended for the information processing provider to perform physical destruction measures themselves. However, if outsourcing to external contractors is necessary, provide the medical institution with the basis for selecting the contractor and obtain approval for the external outsourcing. Additionally, receive and store certificates or other proof that information retrieval has become impossible due to the destruction measures. As for the disposal methods of hard disks, physical destruction measures such as irradiation with magnetic fields of certain strength or melting processing are reliable. However, software-based data wiping methods involving multiple overwrites of random data and fixed patterns (e.g., NSA recommended method, US Department of Defense compliant method, NATO method, Gutmann method, etc.) are also commonly used. Choose an appropriate method based on the importance of the stored information, explain the rational reasons for the selection to the medical institution, obtain agreement, and then proceed with implementation.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Disposal of Media” (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • “Secure disposal or reuse of equipment” (27K1:2013 A.11.2.7; 27K1:2022 A.14). • “Removal of assets” (27K1:2013 A.11.2.5; 27K1:2022 A.7.10) • “Equipment maintenance” (27K1:2013 A.11.2.4; 27K1:2022 A.13). • “Documented Operating Procedures” (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). Information security oversight and management controls, including media security are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis hard drives incorporate technologies such as full-disk encryption (FDE) and drive locking mechanisms to secure data at rest. Acronis uses a software-defined storage solution, which utilizes a proprietary erasure-coding algorithm, and which securely removes customer data. In the case Acronis Cyber Infrastructure drives and equipment are broken, switched out for repair or decommissioned, Acronis takes measures to erase data from a disk and remove residual data from the internal memory of the equipment, according to NIST SP 800-88rev1. In the event that it is not possible to erase (delete) such information, equipment is physically destroyed in such a way that it’s impossible to read (restore) such data. Acronis, within data center colocation, uses local qualified third parties to ensure physical disposal of drives. Customers are solely responsible for evaluating and maintaining their own legal and compliance obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with its customers, who have such obligation under applicable data protection regimes.
		③-9	When disposing of electronic media, apply physical destruction measures such as melting by high temperatures or shredding to ensure that information retrieval is impossible.	
		③-10	The operation management regulations shall define the following: • To periodically confirm the necessity of managing personal information or the media storing it, in the context of providing medical information systems. • The disposal procedures for personal information and the media storing it, deemed unnecessary for the provision of medical information systems. • Measures to prevent unforeseen damage to medical institutions, etc., when disposing of personal information and the media storing it, deemed unnecessary for the provision of medical information systems (such as notifying the criteria for disposal in advance).	
		③-11	Agree with medical institutions about the procedures for destroying information.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	4 Measures for carry out data and equipment outside the offices.	4-1	The company shall establish its own policies and procedures based on the principle that entrusted personal information shall not be stored in terminals used for operation and maintenance.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Equipment siting and protection" (27K1:2022 A.11.2.1; 27K1:2022 A.7.8). • "Equipment maintenance" (27K1:2013 A.11.2.4; 27K1:2022 A.13). • "Security of equipment and assets off-premises" (27K1:2013 A.11.2.6; 27K1:2022 A.7.9). • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10) • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Removal of assets" (27K1:2013 A.11.2.5; 27K1:2022 A.7.10) • "Documented Operating Procedures" (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). Acronis' employees do not have access to customers' content data. Customers' content data is not exported for any reason on Acronis' employee terminals.
		4-2	When it is necessary to take out devices storing medical information for maintenance purposes (such as equipment repair) to organizations outside medical institutions or contracted service provider (including sub-contractors), procedures for such actions shall be established.	
		4-3	Company should agree with medical institutions on the procedures and information provision conditions specified in 4-2.	
		4-4	Establish appropriate verification procedures for reinstalling the removed equipment.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Responsibility for assets" (27K1:2022 A.8.1; 27K1:2022 A.5.9, A.5.10, A.5.11). • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Installation of software on operational systems" (ISO27K1:2013 A.12.5.1; ISO27K1:2022 A.8.19).
		4-5	When troubleshooting is conducted externally and a malfunction or similar issue is found during maintenance and inspection, the operation shall be performed within the jurisdiction managed by the entrusted contractor, so that the troubleshooting operation is not carried out outside. If it is necessary to perform operations outside the designated area, ensure that data within the device is securely erased before removal. For a device such as a storage device where information cannot be erased due to a malfunction, choose disposal after physically destroying the device instead of attempting repair.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Equipment siting and protection" (27K1:2022 A.11.2.1; 27K1:2022 A.7.8). • "Equipment maintenance" (27K1:2013 A.11.2.4; 27K1:2022 A.13). • "Security of equipment and assets off-premises" (27K1:2013 A.11.2.6; 27K1:2022 A.7.9). • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Removal of assets" (27K1:2013 A.11.2.5; 27K1:2022 A.7.10). • "Documented Operating Procedures" (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). Acronis, as an internal policy, doesn't reuse or repair damaged hardware. Damaged hardware is decommissioned. Acronis' employees do not have access to customers' content data. Customers' content data is not exported for any reason on Acronis' employee terminals. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including development of operational procedures and guidelines.
		4-6	The items included in the removal procedure may include the following: • Format of the device removal application form (applicant information, approver information, device information, removal date and time, scheduled return date and time, location to be taken out, reason for removal, overview of information stored in the device, results of risk assessment associated with removal, response measures in case of device loss or damage, etc.) • Application approval process • Return confirmation process, etc.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❹-7	The following items may be included in the verification procedure at the time of return: • Checking equipment operation • Presence of devices threatening information security, such as eavesdropping devices • Detection of malicious programs • Verification of stored information for unauthorized tampering, etc.	
	❺ Establishment of procedures for managing the equipment or media carried out.	❺-1	Policies and Procedures regarding the taking out (including taking out from the commissioning entity) of devices or media storing information related to the service (commissioned information, information related to information systems, etc.) shall be defined in the operational management regulations.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Equipment siting and protection" (27K1:2013 A.11.2.1; 27K1:2022 A.7.8). • "Security of equipment and assets off-premises" (27K1:2013 A.11.2.6; 27K1:2022 A.7.9). • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Removal of assets" (27K1:2013 A.11.2.5; 27K1:2022 A.7.10). • "Documented Operating Procedures" (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). • "Acceptable use of the assets" (27K1:2013 A.8.1.3; 27K1:2022 A.5.10). • "Networks security" (27K1:2013 A.13.1.1; 27K1:2022 A.8.20). • "Information backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). Acronis ensures the encryption and authentication of all data in transit across one or more network layers when the data traverses external boundaries not under Acronis direct control or is transferred on Acronis behalf. Large-capacity electronic media are used only in case a customer requests the Physical Data Shipping service for initial backup. For more information on Physical Data Shipping service refer to: https://www.acronis.com/support/providers/physical-data-shipping/ Acronis hard drives incorporate technologies such as full-disk encryption (FDE) and drive locking mechanisms to secure data at rest. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including development of operational procedures and guidelines.
		❺-2	In "❺-1", "taking out" includes not only physical removal, but also transmission to external parties via network.	
		❺-3	Agree with medical institutions, etc. for the contents defined in "❺-1".	
		❺-4	Do not unnecessarily take electronic media outside the facilities of the entrusted business. This includes CDs, DVDs, MO disks, etc.	
		❺-5	When large-capacity electronic media such as MTs, DATs, solid-state memory devices, and hard disks are used for data interchange and backup purposes, strict management must be implemented. When information is recorded multiple times on these electronic media, measures to prevent information leakage, such as reliable data erasure, should be implemented instead of simply overwriting.	
		❺-6	All electronic media should be labeled to indicate the level of confidentiality of the information being stored.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Classification of information" (27K1:2013 A.8.2.1; 27K1:2022 A.5.12). • "Labeling of information" (27K1:2013 A.8.2.2; 27K1:2022 A.5.13). Customers can apply their own data-labeling standard to information stored in Acronis Cyber Protect Cloud.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❺-7	The following contents regarding recording media and recording devices shall be included in the operational management regulations: • Management system and management method • Usage and maintenance of recording media and equipment • Policies and rules regarding the removal (including removal by the consigner) of equipment, media, etc. that store information related to services (consignment information, information related to information systems, etc.) ("removal" includes not only physical removal but also transmission to the outside through a network). • Handling in the event of theft or loss of equipment/media, etc. that contain information related to services when such information is taken out (including physical theft or loss of equipment/media, etc. when taken out, as well as transmission outside the company that is not approved by the system administrator (including malicious transmission by a third party, erroneous transmission by an employee, etc.)).	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Documented Operating Procedures" (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). • "Information security awareness, education and training" (27K1:2013 A.7.2.2; 27K1:2022 A.6.3). Acronis upholds comprehensive internal documentation and adheres to an Information Security Management System (ISMS), in compliance with ISO 27001 standards. All documents are stored on systems that are replicated and backed up. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including development of operational procedures and guidelines. All Acronis contractors receive security training as an integral part of their induction process and continue to receive training throughout their tenure at Acronis. As part of their orientation, new contractors commit to our Code of Conduct, emphasizing our dedication to protecting customer information securely. Based on their specific roles, they may undergo additional training on particular security facets. For example, the information security team provides new engineers with training on secure coding practices, product design and the use of automated vulnerability testing tools. Information security oversight and management controls, including management of security awareness and training, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report.
		❺-8	Conduct education for employees and contractors on the contents of ❺-7	
		❺-9	Subcontractors are also required to comply with the operational regulations outlined in ❺-7	
	❻ Development of procedures related to quality control of equipment and software.	❻-1	Develop appropriate change management procedures for information processing hardware and software. Ensure that maintenance activities are communicated to medical institutions in advance, allowing sufficient time for approval.	Acronis is certified to the ISO 9001 and ISO/IEC 27001 Standards, which regulate: • "Change management" (27K1:2013 A.12.1.2; 27K1:2022 A.8.32). • "System acquisition, development and maintenance" (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). • "Design and development of products and services" (9001:2015 8.3). Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
		❻-2	Include measures, procedures, and related practices for quality management of equipment and software in the operational management policies and procedures.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❻-3	Conduct quality management training regarding equipment and software for employees and related personnel.	Acronis is certified to the ISO 9001 and ISO/IEC 27001 Standard, which regulate: • "Change management" (27K1:2013 A.12.1.2; 27K1:2022 A.8.32). • "System acquisition, development and maintenance" (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). • "Design and development of products and services" (9001:2015 8.3). Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
		❻-4	For contractors involved with medical information systems demand compliance with quality management practices conducted by our company to meet the requirements of these guidelines.	
		❻-5	The change procedure may encompass the following elements: • A process for notifying stakeholders impacted by the change. • The format of the change application form for equipment, including details such as applicant information, approver information, information about the equipment undergoing change, the start date and duration of the change operations, reason for the change, a summary of the information contained within the equipment, results of the risk assessment related to the change, and countermeasures in case the equipment is damaged, among others. • The process for approving requests. • The process for testing changes. • Procedures for recovery in the event of issues arising during the change operations. • The process for confirming the completion of changes. • A process for monitoring the impacts resulting from the changes.	
1.2 Use of test data not containing personal information.	❶ Measures for the use of data containing personal information.	❶-1	Do not directly use medical information as development and testing data. If such data is to be used, establish data manipulation procedures such as the removal of personally identifiable information and the replacement of parts of the data with random data to prevent the original data from being restored. Ensure that sufficient security measures are in place and demonstrate this to medical institutions and similar entities to obtain their consent before use.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27018 Standards, which regulate: • "Separation of development, testing and operational environments" (27K1:2013 A.12.1.4; 27K1:2022 A.8.31; 27K18:2019 12.1.4). • "Security in development and support processes" (27K1:2013 A.14.2; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
1.3 Contract related to confidentiality obligations.	❶ Contract engagement of confidentiality obligation with all staff for provision of medical information system.	❶-1	Require all staff of contracted service provider who may handle medical information to sign a confidentiality agreement as a condition of their employment contract or upon taking up duties involving medical information. In the case of dispatched employees, select and deploy them on the condition that they are subject to confidentiality obligations and undergo continuous information security training.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Screening" (27K1:2013 A.7.1.1; 27K1:2022 A.6.1). • "Terms and conditions of employment (27K1:2013 A.7.1.2; 27K1:2022 A.6.2). • "Information security awareness, education and training (27K1:2013 A.7.2.2; 27K1:2022 A.6.3). • "Disciplinary process" (27K1:2013 A.7.2.3; 27K1:2022 A.6.4). • "Acceptable use of assets" (27K1:2013 A.8.1.3; 27K1:2022 A.5.10). • "Confidentiality or nondisclosure agreements" (27K1:2013 A.13.2.4; 27K1:2022 A.6.6). • "Remote working" (27K1:2013 A.6.2.2; 27K1:2022 A.6.7). Acronis performs background checks on new hires as permitted by local laws. Information security oversight and management controls, including confidentiality commitment of Acronis, hiring practice controls, management of security awareness and training are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Terms of Service: https://www.acronis.com/support/platform-terms-conditions/ Privacy Statement: https://www.acronis.com/company/privacy/ Acronis End-User License Agreement: https://www.acronis.com/support/eula/
		❶-2	For all contractor staff (including temporary employees) who might handle medical information, it is required to incorporate the details of confidentiality obligations into the work regulations or equivalent documents.	
		❶-3	Establish a ledger and return confirmation procedures beforehand to ensure the complete return of all information assets when staff (including dispatched employees) of a contractor operating medical information leave the company. It is also required to obtain signatures on an agreement that mandates the confidential management of medical information learned during employment, even after departure. For dispatched employees, request a signature on an equivalent agreement at the time of dispatch contract termination.	
		❶-4	Employment contracts, dispatch contracts or work rules should include confidentiality obligations for personal data handled during the work, when the contractor staff (including temporary staff) operating the medical information leaves office.	
		❶-5	Include appropriate disciplinary procedures for staff of subcontractors (including dispatched employees) who violate the aforementioned conditions, in employment or dispatch contracts, or incorporate them into the employment regulations or similar documents. Ensure that the established disciplinary procedures are made known to all staff and confirm their understanding of these procedures.	
		❶-6	Agree with medical institutions and similar entities on providing documentation regarding the implementation of education and training for staff of subcontractors (including dispatched employees) who handle medical information, as well as their compliance with confidentiality obligations and other relevant matters.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	❷ Contract engagement including confidentiality obligations with medical institutions and sub-contractors.	❷-1	Include confidentiality obligations regarding information related to medical information systems and entrusted information in contracts related to the provision of such systems. The contracts should specify that penalties will be imposed on subcontractors who violate these confidentiality obligations and include provisions regarding the supervision by medical institutions and similar entities over the handling of the entrusted information.	Acronis is certified to the ISO/IEC 27017 standard for cloud providers. Information security oversight and management controls, including confidentiality commitment of Acronis, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Terms of Service: https://www.acronis.com/support/platform-terms-conditions/ Privacy Statement: https://www.acronis.com/company/privacy/ Acronis End User License Agreement: https://www.acronis.com/support/eula/
		❷-2	Procedures including confirmation of operations by personnel and consignees for whom confidentiality obligations are imposed should be defined when data including consigned personal data is inevitably used for confirmation of operations of medical information systems.	Not applicable. This is the customer's responsibility to respond to.
		❷-3	Agree with medical institutions and similar entities on the use of entrusted personal information when it is unavoidable during the operation verification of medical information systems and similar.	Not applicable. This is the customer's responsibility to respond to.
1.4. Implementation of education and training.	❶ Implementation of education and training related to the provision of medical information systems and similar services.	❶-1	Provide education on personal information protection and information security to all staff, including subcontractor staff who may handle medical information. Only permit those staff members who have attained a specified level of understanding to participate in related tasks.	Acronis is certified to the ISO 9001 and ISO/IEC 27001 Standards, which regulate: • "Information security awareness, education and training" (27K1:2013 A.7.2.2; 27K1:2022 A.6.3). • "Organizational knowledge", "Competence", "Awareness" (9001:2015 7.1.6, 7.2, 7.3). • "Responsibilities after termination or change of employment" (27K1:2013 A.7.3.1; 27K1:2022 A.6.5). All Acronis contractors receive security training as an integral part of their induction process and continue to receive training throughout their tenure at Acronis. As part of their orientation, new contractors commit to our Code of Conduct, emphasizing our dedication to protecting customer information securely. Based on their specific roles, they may undergo additional training on particular security facets. For example, the information security team provides new engineers with training on secure coding practices, product design, and the use of automated vulnerability testing tools. Information security oversight and management controls, including management of security awareness and training, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report.
		❶-2	For dispatched employees, request the dispatching agency to select and dispatch individuals who possess or are capable of acquiring a certain level of knowledge and understanding regarding personal information protection and information security. After acceptance, provide education equivalent to that of regular staff.	
		❶-3	This education should be conducted regularly in accordance with new threats and the evolution of information security technologies.	
		❶-4	Include confidentiality obligations after resignation or contract termination for staff and subcontractors (including dispatched employees) who handle medical information, in education and training.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
1.5. Monitoring of operational status.	❶ Monitoring of access and manipulation activities within medical information systems and related services.	❶-1	When there is suspicion of a violation of security measures by staff of subcontractors, immediately suspend their access rights to medical information and verify that no acts of tampering or destruction have occurred.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • "Information security incident management planning and preparation" (27K1:2013 A.16.1.1; 27K1:2022 A.5.24). • "Assessments and decisions on information security events" (27K1:2013 A.16.1.4; 27K1:2022 A.5.25). • "Response to information security incidents" (27K1:2013 A16.1.5; 27K1:2022 A.5.26). • "Reporting information security events" (27K1:2013 A.16.1.2; 27K1:2022 A.6.8). Acronis maintains a stringent incident management process dedicated to addressing security incidents that may compromise the confidentiality, integrity or availability of its systems or data. When a security incident is identified, the Acronis security team promptly logs and categorizes the incident according to its severity. Incidents affecting customers directly are given the highest priority. The process details specific actions, notification and escalation procedures, mitigation steps and documentation practices. Regular testing of the incident response plans is conducted, with a special focus on systems containing sensitive customer data. These tests cover various threat scenarios, including internal risks and software vulnerabilities, to ensure the team's readiness. In cases where a security breach involves customer data, Acronis and its partners commit to promptly notifying the affected customers and offering comprehensive support through the investigation process. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment, so as detect unauthorized access and take actions to mitigate it eventually.
		❶-2	When performing maintenance on medical information systems, notifications should be made to administrators of medical institutions, in writing or equivalent means, both before and after the maintenance work as a general rule. Agree with medical institutions on the tasks that require prior consent and on the methods of handling situations where such prior consent cannot be obtained.	Acronis Cyber Protect Cloud services are offered via partnered managed service providers (MSPs). MSPs can enable functionality to notify customers in case of maintenance. If notification functionality is not already available to their customers, they should ask their own MSP to enable this functionality to be notified about maintenance windows that could impact their own operations. For more information please visit: https://kb.acronis.com/content/70368 https://www.acronis.com/en-us/support/ Customers are solely responsible for evaluating and fulfilling their own legal and compliance obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with its customers, who have such obligation under applicable data protection regimes.
		❶-3	After carrying out maintenance work, provide reports to medical institutions and obtain the approval of the institutions' administrators. Agree with medical institutions on the approach for this procedure.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-4	Agree with medical institutions on the procedures for performing maintenance work on medical information systems and similar within the facilities of medical institutions.	Not applicable. This is the customer's responsibility to respond to.
	❷ Regular verification of the location of equipment and media.	❷-1	Manage electronic media by creating and maintaining a ledger. Regularly verify the ledger and electronic media to check for occurrences of theft or loss. Record usage in the ledger and maintain records for a certain period after the disposal of the electronic media.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Responsibility for assets" (27K1:2022 A.8.1; 27K1:2022 A.5.9, A.5.10, A.5.11). • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Installation of software on operational systems" (ISO27K1:2013 A.12.5.1; ISO27K1:2022 A.8.19). Acronis' employees do not have access to customers' content data. Customers' content data is not exported for any reason on Acronis employees' terminals. Acronis hard drives incorporate technologies such as full-disk encryption (FDE) and drive locking mechanisms to secure data at rest. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❷-2	For equipment and media storing information, conduct ledger management and regularly verify their locations.	
		❷-3	Limit the equipment and media storing personal information to the minimum necessary for service provision and operation and conduct regular location checks and inventory audits.	
	❸ Implementation of internal audits regarding system configuration and software operational status.	❸-1	Include the content and procedures of internal audits related to system configuration and software operational status in the operational management policies and procedures.	Acronis is certified to the ISO 9001 and ISO/IEC 27001 Standards, which regulate: • "Change management" (27K1:2013 A.12.1.2; 27K1:2022 A.8.32). • "System acquisition, development and maintenance" (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). • "Design and development of products and services" (9001:2015 8.3). Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
1.6. Measures for physical data transfer.	❶ Measures such as encryption for information taken outside the organization.	❶-1	When physically transporting information, implement the following measures: · Select a trusted delivery service based on criteria agreed upon with medical institutions and similar entities. · Perform identity verification of the dispatch and receiving parties to prevent impersonation by third parties. · To prevent the removal of electronic media by delivery personnel, pre-arrange the exchange of information regarding the number and type of electronic media to ensure no discrepancies at receipt. · Use containers that can detect unauthorized opening to prevent information extraction from electronic media by delivery personnel. · Conduct the shipment and receipt of electronic media directly with the delivery service, without involving third parties. · Encrypt data on electronic media when exchanging information, if there are risks associated with the security management during transit.	Media used to store data will not be transferred outside Acronis data centers. It's possible for Acronis' customers to ship physical media for an initial backup. For more information on this process refer to https://www.acronis.com/support/providers/physical-data-shipping/
1.7. Restrictions on Analysis and Provision to Third Parties.	❶ Restrictions on the analysis and provision of entrusted medical information to third parties.	❶-1	Limit the viewing of entrusted medical information to the minimum necessary for maintenance and operation purposes.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: · "Access Control" (27K1:2013 A.9 ; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). · "Documented Operating Procedures" (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). · "Networks security" (ISO27K1:2013 A.13.1.1, A.13.1.3; ISO27K1:2022 A.8.20, A.8.22). · "Data leakage prevention" (27K1:2022 8.12). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis' employees do not have access to customers' content data. Customers' content data is not exported for any reason on Acronis employees' terminals. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including development of operational procedures and guidelines.
		❶-2	"❶-1 When viewing is necessary, excluding emergencies, it should be carried out with prior and subsequent approval from the system administrator."	
		❶-3	In cases where entrusted medical information is viewed during an emergency, obtain approval from the system administrator by indicating the scope of the information viewed and the reasons why emergency viewing was necessary.	
		❶-4	Agree with medical institutions on the scope and procedures related to viewing under sections ❶-1 to ❶-3. Additionally, promptly report to medical institutions when medical information is viewed in accordance with sections ❶-2 and ❶-3.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-5	Do not conduct analysis or analytics on entrusted medical information, except when commissioned by medical institutions or similar entities based on a contract separate from the contract related to the provision of medical information systems.	Not applicable. This is the customer's responsibility to respond to. Customers' data will always be processed based on the contracted agreement. Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/company/privacy/ https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/support/eula/
		❶-6	Treat information that has been anonymized from entrusted medical information with the same level of care as the original medical information	
		❶-7	Do not provide entrusted medical information to third parties, including the patient themselves, except when required by law or based on instructions from medical institutions or similar entities.	Acronis is certified to the ISO/IEC 27017 and ISO/IEC 27018 standards for cloud providers. Information security oversight and management controls, including confidentiality commitment of Acronis are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/company/privacy/ https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/support/eula/
		❶-8	Include the contents of ❶-7 in contracts related to the provision of medical information systems and similar services.	
		❶-9	When providing (viewing) entrusted medical information to third parties based on instructions from medical institutions, take measures to ensure that no one other than those authorized by the medical institutions can view or obtain the information.	Not applicable. This is the customer's responsibility to respond to. Customers' data will always be processed based on the contracted agreement. Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/company/privacy/ https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/support/eula/
		❶-10	When providing (viewing) to third parties as per ❶-9, follow the instructions of medical institutions or their authorized entities (such as medical information exchange networks) regarding the ID and access rights of those who are allowed to view and obtain the information.	
		❶-11	When providing entrusted medical information to third parties based on instructions from medical institutions, report the details (recipient (viewer), information viewed, date and time of viewing, etc.) to the medical institutions.	
		❶-12	Agree with medical institutions on the conditions and scope for providing to third parties and reporting as per ❶-7 to ❶-11.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
1.8. Submission of Records Related to the Disposal of Information.	❶ Acquisition and submission of implementation records related to the disposal of information to medical institutions or similar entities.	❶-1	When disposal of information is carried out, report to medical institutions or similar entities upon request, including details of the personnel responsible for the implementation and the methods of information deletion (such as demagnetization of magnetic media or physical destruction), and submit records of the disposal.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Removal of assets" (27K1:2013 A.11.2.5; 27K1:2022 A.7.10). • "Equipment maintenance" (27K1:2013 A.11.2.4; 27K1:2022 A.13). • "Documented Operating Procedures" (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). Information security oversight and management controls, including media security, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Acronis uses a software-defined storage solution, which utilizes a proprietary erasure-coding algorithm, and which securely removes customer data. In the case Acronis Cyber Infrastructure drives and equipment are broken, switched out for repair, or decommissioned, Acronis takes measures to erase data from a disk and remove residual data from the internal memory of the equipment, according to NIST SP 800-88rev1. In the event that it is not possible to erase (delete) such information, equipment is physically destroyed in such a way that it's impossible to read (restore) such data. Acronis, within data center colocation, uses local qualified third parties to ensure physical disposal of disks. Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/company/privacy/ https://www.acronis.com/support/eula/
		❶-2	It is preferable for contracted service providers themselves to carry out the destruction of physical electronic media and the disposal of destroyed media. If outsourcing to an external specialist is necessary, provide the rationale for selecting the service provider to medical institutions or similar entities and ensure their full understanding. Additionally, obtain and retain certificates or similar documents proving that the information on the destroyed media cannot be retrieved as a result of the destruction measures.	
		❶-3	Agree with medical institutions or similar entities on the conditions necessary for implementing the measures and providing the documentation as per ❶-1.	
		❶-4	In the event of a cessation of the provision of medical information systems or a suspension of use by medical institutions or similar entities, promptly proceed with the deletion of records and disposal of media, among other actions. Upon completing the deletion of records and disposal of media, submit documentation to the medical institutions or similar entities to certify these actions.	
		❶-5	For ❶-4, when retaining records within the minimum necessary scope for providing support to medical institutions (including the submission of information to regulatory authorities), it is important to reach an agreement with the medical institutions or similar entities on the objectives, scope, duration of retention, methods for managing the records, safety management measures, and contact information.	Not applicable. This is the customer's responsibility to respond to. Customers' data will always be processed based on the contracted agreement. Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/company/privacy/ https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/support/eula/

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
1.9. Management of Subcontractors.	❶ Informing medical institutions or similar entities when subcontracting and ensuring appropriate supervision of the subcontracted party.	❶-1 ❶	When subcontracting tasks related to information systems, provide explanations in advance to administrators of medical institutions or similar entities and obtain their agreement. Additionally, clarify the system in the contract related to the subcontracting.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • "Supplier Relationships" (27K1:2013 A.15; 27K1:2022 A.5.19, A.5.20, A.5.21, A.5.22; 27K17 15). Information security oversight and management controls, including vendors' security practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Before onboarding third-party suppliers, Acronis carries out a thorough evaluation of the security and privacy measures implemented by these suppliers. This assessment ensures that the suppliers uphold a standard of security and privacy that aligns with the data access levels and the breadth of services they are contracted to deliver. Following the risk assessment of a third-party supplier by Acronis, the supplier is mandated to agree to specific contract terms covering security, confidentiality and privacy. Acronis' Data Protection Addendum (DPA) describes the terms and process for customers to object to subprocessor changes.
		❶-2	Ensure that subcontracted parties adhere to personal information protection policies equivalent to those of your own company.	
		❶-3	Include confidentiality obligations related to the outsourced tasks in the contract for subcontracting.	
		❶-4	Confirm that personnel at the subcontracted party have confidentiality obligations equivalent to those of your own company.	
		❶-5	Agree with medical institutions or similar entities on the scope, content, and conditions for providing information regarding reports to be made when there are changes in the system for maintenance of medical information systems and similar.	Customers are solely responsible for evaluating and maintaining their own legal and compliance obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with its customers, who have such obligation under applicable data protection regimes.
		❶-6	When outsourcing part or all of the maintenance of medical information systems to an external service provider, require that the service provider adheres to the operational management policies and safety management measures that are implemented within your own company.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • "Supplier Relationships" (27K1:2013 A.15; 27K1:2022 A.5.19, A.5.20, A.5.21, A.5.22; 27K17 15). Information security oversight and management controls, including vendors' security practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Before onboarding third-party suppliers, Acronis carries out a thorough evaluation of the security and privacy measures implemented by these suppliers. This assessment ensures that the suppliers uphold a standard of security and privacy that aligns with the data access levels and the breadth of services they are contracted to deliver. Following the risk assessment of a third-party supplier by Acronis, the supplier is mandated to agree to specific contract terms covering security, confidentiality and privacy. Acronis, according to its risk evaluation for a third-party vendor, periodically performs reassessment of the security posture of the vendor itself. Acronis includes a Data Protection Addendum (DPA) in agreements with third-party subprocessors that might access customer data. This DPA outlines the security and privacy responsibilities the subprocessor must fulfill to meet Acronis' commitments concerning the protection of customer data.
		❶-7	Regarding the implementation of ❶-6, request and verify reports from external service providers either after each contract execution or on a regular basis.	
		❶-8	Ensure that the safety management measures and service level provided by the subcontracted party for medical information systems are sufficient.	
		❶-9	Regularly verify the implementation, operation, and maintenance of medical information systems by the subcontracted party.	
		❶-10	Periodical reports on implementation, operation and maintenance of services carried out by subcontractors should be provided beforehand and afterwards, and the report should be checked and confirmed by the provider.	
		❶-11	Personnel to carry out the medical information system, such as staff of subcontractor must request access in advance and do not accept unauthorized personnel when carrying out the service.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-12	When subcontracting tasks related to information systems, provide explanations in advance to administrators of medical institutions or similar entities and obtain their agreement. Additionally, clarify the system in the contract related to the subcontracting.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). Information security oversight and management controls, including physical security management practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report.
		❶-13	Regarding the entry procedures into the processing facilities accompanying the implementation of medical information systems by the subcontracted party, adhere to the entry and exit procedures of the contracted service provider's staff.	
		❶-14	When changes are made to medical information systems by the subcontracted party, conduct appropriate verification to ensure that safety is continuously maintained.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • "Supplier Relationships" (27K1:2013 A.15; 27K1:2022 A.5.19, A.5.20, A.5.21, A.5.22; 27K17 15). Information security oversight and management controls, including vendors' security practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report.
		❶-15	When outsourcing maintenance and inspection work of medical information systems to an external service provider, implement management measures in accordance with the safety management measures for maintenance responses by medical information system & service providers, as outlined in the guidelines for the safe management of medical information systems, System Operation Edition, "10. Safety Management Measures for Maintenance Responses by Medical Information System & Service Providers."	Not applicable. This is the customer's responsibility to respond to.
		❶-16	When an external service provider carries out work on medical information systems, it is preferable that the work is performed under the supervision of regular staff from either the contracted service provider or the external service provider.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • "Supplier Relationships" (27K1:2013 A.15; 27K1:2022 A.5.19, A.5.20, A.5.21, A.5.22; 27K17 15). Information security oversight and management controls, including vendors' security practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
1.10. Measures for Emergency Preparation.	① Perform of a business impact analysis related to the provision of medical information systems.	①-1	Identify business processes related to medical information processing (including the workers who carry out these processes) and information processing equipment.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39). • "ICT readiness for business continuity" (27K1:2022 A.5.30). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers' content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data, and if available, enable additional georedundancy services according to their own business continuity and disaster recovery strategies. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/
		①-2	Evaluate the interrelationships between business processes.	
		①-3	To prioritize business processes for continuity, clarify their order of importance.	
		①-4	Identify the impact of hardware and software failures in medical information systems on business processes.	
		①-5	Recognize the impact and interaction of hardware and software failures in medical information systems on other hardware and software, and identify hardware and software with significant impact.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	❷ Planning and verification through simulated tests for business continuity in the provision of medical information systems.	❷-1	Develop a business continuity plan for medical information processing, incorporating the perspective of healthcare continuity as envisioned by medical institutions in the provision of medical information systems and related services.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39). • "ICT readiness for business continuity" (27K1:2022 A.5.30). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Business continuity plans are designed and regularly carried out for both offices and data center colocations. Acronis does not duplicate customers' content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data, and if available, enable additional georedundancy services according to their own business continuity and disaster recovery strategies. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/ Customers are solely responsible for evaluating and maintaining their own legal and compliance obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with its customers, who have such obligation under applicable data protection regimes.
		❷-2	Review the developed business continuity plan, including conducting simulation exercises, using appropriate methods.	
		❷-3	Periodically review the business continuity plan.	
		❷-4	The following items are desirable to include in the drafted business continuity plan: • Preparatory measures • Procedures for determining "emergency" situations • Summoning relevant personnel and establishing response headquarters • Contingency measures for equipment and personnel reduction, as well as arrangements for alternative facilities • Procedures for switching to backup facilities or alternative sites • Considerations during the operation of alternative facilities (such as operating procedures for emergency accounts, and considerations for synchronizing medical information with the normal system after recovery) • Procedures and criteria for assessing the scope of the disturbance • Procedures and criteria for determining normal recovery • Checking procedures for medical information systems and other systems after normal recovery (detection of unauthorized access, information tampering, data corruption, etc.) • Communication protocols with relevant authorities	
		❷-5	Agree on the service content based on the formulated business continuity plan with medical institutions and other relevant stakeholders.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	3 Ensuring data integrity after the restoration of medical information systems and other related systems.	3-1	Measures should be taken to ensure data integrity to prevent discrepancies in data processing results during emergencies from occurring after service recovery. This may include the establishment of policies and procedures for verification methods.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39). • "ICT readiness for business continuity" (27K1:2022 A.5.30). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including development of a business continuity and disaster recovery strategies.
	4 Procedures should be established for managing user accounts and functionalities specifically for emergency situations	4-1	Agree with the medical institutions on the measures to enable emergency user accounts and emergency functions.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39). • "ICT readiness for business continuity" (27K1:2022 A.5.30). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers' content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data, and if available, enable additional georedundancy services according to their own business continuity and disaster recovery strategies. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/.
		4-2	Periodic reviews will be made on the status of use of user accounts in emergency situations.	
		4-3	When the emergency user accounts are used, measures should be taken to enable the system administrator and operator to promptly confirm this.	
		4-4	For the user accounts and emergency functions that were activated during the emergency, they should be disabled promptly upon returning to normal status.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
1.11. Response to Incidents Caused by Cyber Attacks.	❶ Immediate Reporting to Medical Institutions in the Event of Cyber Attack Incidents.	❶-1	In the event of service disruption due to cyber attacks or similar incidents, promptly report to medical institutions regarding the status of the service disruption and the outlook for recovery.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: · "Information security incident management planning and preparation" (27K1:2013 A.16.1.1; 27K1:2022 A.5.24). · "Assessments and decisions on information security events" (27K1:2013 A.16.1.4; 27K1:2022 A.5.25). · "Response to information security incidents" (27K1:2013 A16.1.5; 27K1:2022 A.5.26). · "Reporting information security events" (27K1:2013 A.16.1.2; 27K1:2022 A.6.8). Information security oversight and management controls, including incidents management practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis maintains a stringent incident management process dedicated to addressing security incidents that may compromise the confidentiality, integrity or availability of its systems or data. When a security incident is identified, the Acronis security team promptly logs and categorizes the incident according to its severity. Incidents affecting customers directly are given the highest priority. The process details specific actions, notification and escalation procedures, mitigation steps and documentation practices. Regular testing of the incident response plans is conducted, with a special focus on systems containing sensitive customer data. These tests cover various threat scenarios, including internal risks and software vulnerabilities, to ensure the team's readiness. In cases where a security breach involves customer data, Acronis and its partners commit to promptly notifying the affected customers and offering comprehensive support through the investigation process. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-2	In the event of service disruption due to cyber attacks or similar incidents, the scope and conditions for providing materials necessary for medical institutions to contact and report to the relevant administrative authorities shall be agreed upon with the medical institutions. In cases of cyber attacks or other crisis management situations at medical institutions, where the contracted service provider has entered into contracts with medical institutions regarding medical information systems or other matters, the service provider shall specify in the operational management regulations the framework (whether the establishment of an internal crisis response system is necessary, responsible parties, etc.) and its contents (methods of information provision, assessment of the need for role assignment, etc.) to be implemented in accordance with the crisis management response to medical institutions.	
		❶-3	The applications, platforms, servers, storage, etc., used for providing services shall be installed in locations where the enforcement of domestic laws applies, to facilitate the smooth submission of materials that medical institutions are required to submit to the relevant administrative authorities based on legal requirements.	
	❷ Preservation of records such as logs for investigating the cause of cyber attacks or similar incidents.	❷-1	Implement measures to preserve logs and other records necessary for investigating the causes of service disruptions resulting from cyber attacks or similar incidents.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: · "Logging" (27K1:2013 A.12.4; 27K1:2022 A.8.15). · "Monitoring Activities" (27K1:2022 A.8.16). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
1.12. Agreement on Network Responsibilities and Roles.	❶ Agreement on the Scope of Responsibility and Roles When Exchanging Medical Information with External Parties.	❶-1	Agree with medical institutions on the scope of the contracted service provider's role regarding protective measures against tampering, such as the insertion of viruses or unauthorized messages, in network routes.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Protection against malware" (27K1:2013 A.12.2; 27K1:2022 A.8.7). • "Monitoring Activities" (27K1:2022 A.8.16). • "Assessments and decisions on information security events" (27K1:2013 A.16.1.4; 27K1:2022 A.5.25). • "Response to information security incidents" (27K1:2013 A16.1.5; 27K1:2022 A.5.26). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report.
		❶-2	Agree with medical institutions on the scope of the contracted service provider's role regarding protective measures against tampering, such as the insertion of viruses or unauthorized messages, in network routes.	
		❶-3	Agree with medical institutions on the division of roles and responsibilities of the contracted service provider regarding the configuration of routing to prevent transmission between facilities via VPN connected through routers within healthcare facilities used in the network.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). Acronis' employees do not have access to customers' content data. Customers' content data is not exported for any reason on Acronis employees' terminals. Access to the systems responsible for storing or processing this data, is granted following the principle of least privilege. Authentication for access systems and network devices requires a user ID, password, security key, and/or certificate. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including development of operational procedures and guidelines.
		❶-4	Agree with the medical institutions on the scope of responsibility and roles of the contracted service provider specifically for the management and quality assurance of the network.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Communications security" (27K1:2013 A.13; 27K1:2022 A.8.20, A.8.21, A.8.22, A.5.14, A.6.6). • "Securing application services on public networks" (27K1:2013 A.14.1.2; 27K1:2022 A.8.26). Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-5	The responsibility and management procedures of the contracted service provider regarding the network routes and related equipment, as defined in the guidelines for the safe management of the healthcare information system, specifically in the “Network Security Management Measures” section of the System Operation Guidelines, from the starting point to the endpoint of communication procedures during normal and emergency operations between medical institutions and the contracted service provider, should be clearly delineated. Agreement on the location and methods of management responsibility assumed by the contracted service provider should be reached with the medical institutions.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Communications security” (27K1:2013 A.13; 27K1:2022 A.8.20, A.8.21, A.8.22, A.5.14, A.6.6). • “Securing application services on public networks” (27K1:2013 A.14.1.2; 27K1:2022 A.8.26). Acronis’ certifications to the ISO/IEC 27017 and ISO/IEC 27018 Standards assure its commitment to secure its cloud services and a secure handling of PII into the cloud. Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/company/privacy/ https://www.acronis.com/support/eula/
		❶-6	Agree with the medical institutions on the security level of the information to be exchanged, so that the security level will not be lowered at the receiving side.	
		❶-7	Agree with the medical institutions on the contracted service provider’s scope of responsibility and roles regarding the accountability and management responsibilities of medical institution managers to patients.	Customers are solely responsible for evaluating and maintaining their own legal and compliance obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with its customers, who have such obligation under applicable data protection regimes.
		❶-8	Agree with the medical institutions on the conditions and content of security measures that the contracted service provider should implement when providing patient access to medical information managed by the service.	Not applicable. This is the customer’s responsibility to respond to.
		❶-9	Agree with the medical institutions to ensure that the confidentiality level of exchanged information is not lowered at the receiving end.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Communications security” (27K1:2013 A.13; 27K1:2022 A.8.20, A.8.21, A.8.22, A.5.14, A.6.6). • “Securing application services on public networks” (27K1:2013 A.14.1.2; 27K1:2022 A.8.26). Acronis’s certifications to the ISO/IEC 27017 and ISO/IEC 27018 Standards assure its commitment to secure its cloud services and a secure handling of PII into the cloud. Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/company/privacy/ https://www.acronis.com/support/eula/

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-10	Agree with the medical institutions on the contracted service provider's scope of responsibility and roles in the medical institution's managers' accountability and management responsibility for patient information.	Customers are solely responsible for evaluating and maintaining their own legal and compliance obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with its customers, who have such obligation under applicable data protection regimes.
1.13. Quality Management of Equipment and Software.	❶ Documenting the network diagram and specification related to medical information system.	❶-1	Create a configuration diagram for the equipment and software in the medical information system.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). • "Responsibility for assets" (27K1:2022 A.8.1; 27K1:2022 A.5.9, A.5.10, A.5.11). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-2	Create a network configuration diagram for the medical information system.	
		❶-3	Prepare documents with descriptions of system requirements for the devices included in the configuration diagrams created in ❶-1 and ❶-2.	
		❶-4	Create documentation regarding the specifications for updates to the equipment and software comprising the medical information system, as well as their update history.	
		❶-5	Agree with medical institutions on the disclosure content, scope, conditions, etc., for submitting the documents prepared in ❶-1 to ❶-4 upon request from the medical institutions.	
	❷ Implementation of pre-verification for the introduction or modification of equipment and software.	❷-1	Assess the impact of changes to information processing equipment and software resulting from maintenance.	Acronis is certified to the ISO 9001 and ISO/IEC 27001 Standards, which regulate: • "Change management" (27K1:2013 A.12.1.2; 27K1:2022 A.8.32). • "System acquisition, development and maintenance." (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). • "Design and development of products and services" (9001:2015 8.3). Acronis established a Security Development Life Cycle (SDLC) to assure multiple software security checks from design to deployment. A bug bounty program is run to involve independent security researchers. Information security oversight and management controls, including change management and software developing, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
		❷-2	Consider measures to minimize impact and ensure safe data storage when changes may adversely affect existing operations and equipment.	
		❷-3	Applications developed by information service providers themselves should be used for information processing. When an application development by an external developer is used, the application should be used after the safety has been fully verified in advance.	
		❷-4	It is recommended to conduct verification processes at both the binary code level and the source code level to ensure that no malicious programs are included in the software.	
		❷-5	Introduce software and operating system software for business use after conducting sufficient testing.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-10	Agree with the medical institutions on the contracted service provider's scope of responsibility and roles in the medical institution's managers' accountability and management responsibility for patient information.	Customers are solely responsible for evaluating and maintaining their own legal and compliance obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with its customers, who have such obligation under applicable data protection regimes.
1.13. Quality Management of Equipment and Software.	❶ Documenting the network diagram and specification related to medical information system.	❶-1	Create a configuration diagram for the equipment and software in the medical information system.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). • "Responsibility for assets" (27K1:2022 A.8.1; 27K1:2022 A.5.9, A.5.10, A.5.11). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-2	Create a network configuration diagram for the medical information system.	
		❶-3	Prepare documents with descriptions of system requirements for the devices included in the configuration diagrams created in ❶-1 and ❶-2.	
		❶-4	Create documentation regarding the specifications for updates to the equipment and software comprising the medical information system, as well as their update history.	
		❶-5	Agree with medical institutions on the disclosure content, scope, conditions, etc., for submitting the documents prepared in ❶-1 to ❶-4 upon request from the medical institutions.	
	❷ Implementation of pre-verification for the introduction or modification of equipment and software.	❷-1	Assess the impact of changes to information processing equipment and software resulting from maintenance.	Acronis is certified to the ISO 9001 and ISO/IEC 27001 Standards, which regulate: • "Change management" (27K1:2013 A.12.1.2; 27K1:2022 A.8.32). • "System acquisition, development and maintenance." (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). • "Design and development of products and services" (9001:2015 8.3). Acronis established a Security Development Life Cycle (SDLC) to assure multiple software security checks from design to deployment. A bug bounty program is run to involve independent security researchers. Information security oversight and management controls, including change management and software developing, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
		❷-2	Consider measures to minimize impact and ensure safe data storage when changes may adversely affect existing operations and equipment.	
		❷-3	Applications developed by information service providers themselves should be used for information processing. When an application development by an external developer is used, the application should be used after the safety has been fully verified in advance.	
		❷-4	It is recommended to conduct verification processes at both the binary code level and the source code level to ensure that no malicious programs are included in the software.	
		❷-5	Introduce software and operating system software for business use after conducting sufficient testing.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	❸ Separation of production environment and development environment.	❸-1	When developing software, use development environments to avoid the effects on other operating software.	Acronis is certified to the ISO 9001 and ISO/IEC 27001 Standards, which regulate: • “Separation of development, test and production environments” (27K1:2013 A.12.1.4; 27K1:2022 A.8.31). • “System acquisition, development and maintenance.” (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.31, A.8.32). • “Design and development of products and services” (9001:2015 8.3). Acronis established a Security Development Life Cycle (SDLC) to assure multiple software security checks from the design to the deployment. A bug bounty program is run to involve independent security researchers. Information security oversight and management controls, including change management and software developing, are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment.
		❸-2	To prevent the infiltration of malicious programs in the development environment, appropriate measures against malicious programs should be implemented when connected to networks used by the public (such as the internet).	
		❸-3	Do not copy medical information stored in operation environments to development and testing environments.	
		❸-4	To avoid confusion in the operational system, development tools such as development code or compilers should not be placed on the operational system.	
		❸-5	Do not place unnecessary files or data on the operational system for information processing.	
1.14. Minimizing the impact on medical institutions associated with changes.	❶ Support for devices and software used in medical information systems and related components.	❶-1	Regularly verify that the readability of devices, media, etc., storing medical information is maintained.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Information Security during disruption” (27K1:2013 A.17.1; 27K1:2022 A.5.39). • “ICT readiness for business continuity” (27K1:2022 A.5.30). • “Information Backup” (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • “Redundancy of information processing facilities” (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This “redundancy in all aspects” strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers’ content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data according to their own business continuity and disaster recovery strategies. If available, an additional georedundancy service can be enabled. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/.
		❶-2	When there is a possibility that ensuring the readability of devices and media storing entrusted medical information becomes difficult (due to media degradation, end of support for reading devices, etc.), promptly take alternative measures and implement actions to maintain readability.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-3	Each device is maintained and inspected at intervals and according to specifications designated by the manufacturer or supplier, and if necessary, replaced.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Disposal of Media” (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • “Secure disposal or reuse of equipment” (27K1:2013 A.11.2.7; 27K1:2022 A.14). • “Removal of assets” (27K1:2013 A.11.2.5; 27K1:2022 A.7.10) • “Equipment maintenance” (27K1:2013 A.11.2.4; 27K1:2022 A.13). • “Documented Operating Procedures” (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). Information security oversight and management controls, including media security, are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report.
		❶-4	For devices related to information systems, regularly conduct inspections on their deterioration condition and take necessary measures.	Acronis is certified to the ISO 9001 and ISO/IEC 27001 Standards, which regulate: • “Change management” (27K1:2013 A.12.1.2; 27K1:2022 A.8.32). • “System acquisition, development and maintenance.” (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). • “Design and development of products and services” (9001:2015 8.3). Information security oversight and management controls, including change management and software developing, are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
		❶-5	In the event of support termination by providers of devices, software, etc., related to medical information systems, analyze the impact scope on services and take necessary measures.	Acronis’ Platform Terms of Service delineates contractual responsibilities and agreements. Please refer to section 14 and 15 of https://www.acronis.com/en-us/support/platform-terms-conditions/.
		❶-6	In cases where the degradation of devices or the termination of support for devices and software by providers makes it difficult to provide some or all services related to medical information systems, or when changes occur in the services, take measures to minimize the impact on the medical institutions utilizing them. Additionally, provide sufficient notice to these medical institutions to allow them to respond appropriately.	
		❶-7	Agree with the medical institutions on the details and conditions of the response to medical institutions when some or all of the services are stopped or changed under the circumstances described in ❶-6.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	❷ Minimize the downtime of medical information systems due to maintenance work.	❷-1	Plan and implement maintenance work of the information processing apparatus and software so as to minimize the stop time of the information processing work.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Removal of assets" (27K1:2013 A.11.2.5; 27K1:2022 A.7.10). • "Equipment maintenance" (27K1:2013 A.11.2.4; 27K1:2022 A.13). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including controls related to availability and integrity of the systems are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection.
		❷-2	In advance notifications for maintenance work, specify the scope of the impact of the maintenance work and include an estimate of the time required for restoration to the original state, considering the possibility that the maintenance work may not be completed.	
		❷-3	When conducting maintenance work, take sufficient measures to prevent medical institutions from being unable to use the services, and include those procedures in the operational management regulations.	
		❷-4	Present the procedures specified in ❷-3 to the medical institutions for their review, and then reach an agreement on these procedures as well as on the necessary items for conducting maintenance based on them.	
		❷-5	Reach an agreement with the medical institutions on the procedures mentioned in ❷-3, if there are matters that the medical institutions are responsible for addressing.	
	❸ Response to the suspension or specification changes of medical information systems and related technologies.	❸-1	When a part or all of the service is stopped or the service is changed (minor version upgrades are not included), take measures to minimize the impact on the medical institutions using the service, and notify them with a sufficient period for the medical institutions to respond.	Acronis' Platform Terms of Service delineates contractual responsibilities and agreements. Please refer to section 14 and 15 of https://www.acronis.com/en-us/support/platform-terms-conditions/.
		❸-2	Return the entrusted medical information to medical institutions in case of ❸-1. Agree on the range of data to be returned (data type, period, etc.), data format (data item, item details, file format), return method, and conditions with the medical institutions. When the contents of the agreement are changed after the start of service use by medical institutions or other institutions, countermeasures are taken in accordance with ❸-1.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • "Return of the assets" (27K1:2013 A.8.1.4; 27K1:2022 A.5.11). • "Removal of cloud service customer assets" (27K17:2015 CLD.8.1.5). Acronis' Platform Terms of Service delineates contractual responsibilities and agreements. Please refer to section 9.7 of https://www.acronis.com/support/platform-terms-conditions/ .

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❸-3	Regarding the return of data in ❸-2, it shall be conducted in accordance with the guidelines on the safe management of medical information systems, "System Operation Edition 5.1 Importance of Interoperability and Standardization in Medical Information Systems, etc.," and the content thereof will be agreed upon with the medical institutions, etc. Note that the returned data may include data that has undergone irreversible compression (such as image data) or conversion (such as passwords) performed by the entrusted business operator, and this should also be agreed upon with the medical institutions, etc.	
		❸-4	In the event of a partial or complete shutdown of medical information systems, etc., including changes to the service (excluding minor version upgrades) as specified in ❸-1, agree with the medical institutions on the content of the response (such as migration support, excluding the measures in ❸-2) and the conditions.	
		❸-5	When the usage of medical information systems by medical institutions is terminated due to the circumstances of those institutions, implement the measures outlined in ❸-2 and ❸-3	
		❸-6	Include the procedures for ❸-1 to ❸-5 in the operational management regulations and related documents.	
2. Physical Measures				
2.1. Access Control Management.	❶ Authentication and access control for the locations where devices and media are installed.	❶-1	Control the access to and from the security boundaries of the locations where devices and media are installed, based on a personal authentication system or similar controls, to enable the identification of individuals entering and leaving. If this is difficult to achieve, for example, change the passwords or other credentials required for entry and exit on a weekly basis to identify those entering and exiting.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). Information security oversight and management controls, including physical security management practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. To learn more about Acronis' data center security posture, please refer to https://www.acronis.com/resource-center/resource/acronis-cloud-data-centers-a-primer-on-security-privacy-and-compliance/.
		❶-2	Restrict access to the locations where devices and media are installed so that only authorized individuals can enter and exit.	
		❶-3	To restrict access to rooms where medical information systems are installed and medical information is stored, install either manned reception areas, mechanical authentication devices, or both, to ensure reliable authentication of individuals entering and exiting the building and rooms.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-4	When managing individuals entering and exiting without a manned reception, use authentication devices that utilize multiple factors, including at least one biometric authentication method.	
		❶-5	In both cases of manned reception and mechanical access control, acquire authentication records and regularly verify these records to confirm that there are no suspicious activities.	
		❶-6	Specify the duration of time that contracted business operator's staff can stay in the office based on their work duties.	
		❶-7	For authentication factors used in mechanical authentication devices, it is desirable to combine hardware tokens or IC cards and other authentication devices, memorized elements such as PINs or passwords, and biometric information (biometrics), among others.	
		❶-8	Regularly manage the access status to the locations where devices and media are installed, including the review of access records.	
2.2. Lock Management and Key Control.	❶ Lock management and key control for server racks and cabinets.	❶-1	When installing medical information systems, in areas exclusively used by the contracted business operator, apply the following physical security measures. Even when utilizing data centers and server environments operated by external businesses (dedicated servers, virtual private servers, etc.), ensure that equivalent measures are in place. • To prevent unauthorized access to server equipment where medical information is stored, implement lock management and key control for server racks.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). • "Equipment siting and protection" (27K1:2022 A.11.2.1; 27K1:2022 A.7.8). • "Responsibility for assets" (27K1:2022 A.8.1; 27K1:2022 A.5.9, A.5.10, A.5.11). • Physical security for colocated data centers is responsibility shared with each data center facility. Acronis has established partnerships that run numerous global, colocated data center facilities. These facilities meet rigorous standards and compliance needs regarding setup, power and cooling. This approach maintains optimal conditions and uptime to safeguard mission-critical data. Additionally, Acronis has strict requirements for data center locations to reduce or eliminate the probability of the most typical disruptive events. During the term of each contract, Acronis regularly monitors and reviews the third party's security controls, service delivery and compliance with contractual requirements. Information security oversight and management controls, including physical security management practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. To learn more about Acronis' data center security posture, please refer to https://www.acronis.com/resource-center/resource/acronis-cloud-data-centers-a-primer-on-security-privacy-and-compliance/.
		❶-2	Implement lock management for the security boundaries of the locations where devices, media, etc., are installed.	
		❶-3	To restrict access to rooms where medical information systems are installed and medical information is stored, install either manned reception areas, mechanical authentication devices, or both, to ensure reliable authentication of individuals entering and exiting the building and rooms.	
		❶-4	When managing individuals entering and exiting without a manned reception, use authentication devices that utilize multiple factors, including at least one biometric authentication method.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-5	For cabinets storing electronic media, install physical locking devices with sufficient security strength and give careful consideration to key management.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). • "Equipment siting and protection" (27K1:2022 A.11.2.1; 27K1:2022 A.7.8). • "Responsibility for assets" (27K1:2022 A.8.1; 27K1:2022 A.5.9, A.5.10, A.5.11). • Physical security for colocated data centers is responsibility shared with each data center facility. Acronis has established partnerships that run numerous global, colocated data center facilities. These facilities meet rigorous standards and compliance needs regarding setup, power and cooling. This approach maintains optimal conditions and uptime to safeguard mission-critical data. Additionally, Acronis has strict requirements for data center locations to reduce or eliminate the probability of the most typical disruptive events. During the term of each contract, Acronis regularly monitors and reviews the third party's security controls, service delivery and compliance with contractual requirements. Information security oversight and management controls, including physical security management practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. To learn more about Acronis' data center security posture, please refer to https://www.acronis.com/resource-center/resource/acronis-cloud-data-centers-a-primer-on-security-privacy-and-compliance/.
		❶-6	Confirm that external operators running data centers implement safety management measures equivalent to those in their own exclusive buildings, ensuring sufficient security against physical tampering by individuals outside the control of the contracted business operator.	
		❶-7	Lock the server racks where medical information systems, etc., are installed, and ensure reliable key management so that staff other than those designated by the contracted business operator do not handle the keys.	
		❶-8	For work performed by the contracted business operator on server racks where medical information systems, etc., are installed and unlocked, record the worker, start time of work, end time of work, and details of the work performed.	
		❶-9	When external operators running data centers unlock server racks to perform work, it is a principle to provide prior notice and confirm that the work will not affect medical information systems, etc., or the medical information itself.	
		❶-10	Ensure that the fact that it is a medical information system, etc., cannot be identified by other operators entering the same data center, by not making information that can identify the type of information handled or the functions of the system visible from the outside.	
		❶-11	For the locking devices on server racks where medical information systems, etc., are installed, it is desirable to combine authentication devices such as hardware tokens or IC cards, memorized elements like PINs or passwords, and biometric information (biometrics).	
		❶-12	Ensure that sufficient security is in place to protect against unauthorized access by individuals outside the control of the contracted service provider.	
		❶-13	Ensure that information which could reveal the type of information being handled or the functions of the system, including the locations where devices and media are stored (such as racks and cabinets), is not visible from the outside.	
		❶-14	Define items ❶-1 to ❶-13 within the operational management policies and associated documentation.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
2.3. Monitoring for Unauthorized access.	1 Monitoring for intrusion into facilities where medical information is processed, using security cameras and similar equipment.	1-1	When installing medical information systems, etc., in areas exclusively used by the contracted service provider, implement the following physical security measures. Ensure that equivalent measures are taken even when utilizing data centers and server environments operated by external businesses (dedicated servers, virtual private servers, etc.): - To prevent unauthorized acts such as interception and unauthorized filming, ensure walls, ceilings, and floors dividing the rooms have sufficient thickness. Implement measures such as continuous monitoring with surveillance cameras, storage of video recordings, and regular detection of devices installed without authorization. - To deter unauthorized physical intrusion into the building and rooms, introduce intrusion detection devices such as surveillance cameras.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: - "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). Information security oversight and management controls, including physical security management practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. To learn more on Acronis' data center security posture, please refer to https://www.acronis.com/resource-center/resource/acronis-cloud-data-centers-a-primer-on-security-privacy-and-compliance/.
		1-2	Record surveillance footage from security cameras and similar devices, manage it for a specified period, and take measures to ensure it can be referred to afterwards if necessary.	
		1-3	Install surveillance cameras and similar devices in the locations where devices and media are physically stored, save their recordings, and verify the situation to ensure there are no unauthorized entries or exits.	
		1-4	Appropriately monitor areas where service operation and maintenance terminals, etc., are installed using surveillance cameras and similar devices.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	2 Mandate the wearing of employee badges or similar identification by the staff of the contracted service provider.	2-1	If necessary for the continuity of medical information systems provided to medical institutions, establish backup facilities for the medical information entrusted and alternative information processing facilities to continue the medical information systems. Implement physical security measures for these facilities as well.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39). • "ICT readiness for business continuity" (27K1:2022 A.5.30). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices and physical security management are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers' content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data according their own business continuity and disaster recovery strategies; if available, additional georedundancy services can be enabled. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/. To learn more about Acronis' data center security posture, please refer to https://www.acronis.com/resource-center/resource/acronis-cloud-data-centers-a-primer-on-security-privacy-and-compliance/.
		2-2	Staff of the contracted service provider should verbally engage and verify the identity of anyone identified as not being staff of the contracted service provider while in areas exclusively used by the contracted service provider.	
		2-3	When there is suspicion of loss or unauthorized use of an employee badge, immediately contact the manager. Ensure strict issuance and invalidation management of employee badges, including the certain collection and disposal of employee badges upon the resignation of staff of the contracted service provider.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
2.4. Measures at Backup Facilities.	① Implementation of physical security measures for backup facilities.	①-1	If necessary for the continuity of medical information systems provided to medical institutions, establish backup facilities for the medical information entrusted and alternative information processing facilities to continue the medical information systems. Implement physical security measures for these facilities as well.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Physical and environmental security” (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). • “Information Security during disruption” (27K1:2013 A.17.1; 27K1:2022 A.5.39). • “ICT readiness for business continuity” (27K1:2022 A.5.30). • “Information Backup” (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • “Redundancy of information processing facilities” (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including Business continuity practices and physical security management are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This “redundancy in all aspects” strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers’ content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data according their own business continuity and disaster recovery strategies; if available, additional georedundancy services can be enabled. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/. To learn more about Acronis’ data center security posture, please refer to https://www.acronis.com/resource-center/resource/acronis-cloud-data-centers-a-primer-on-security-privacy-and-compliance/.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
2.4. Measures at Backup Facilities.	❶ Implementation of physical security measures for backup facilities.	❶-1	If necessary for the continuity of medical information systems provided to medical institutions, establish backup facilities for the medical information entrusted and alternative information processing facilities to continue the medical information systems. Implement physical security measures for these facilities as well.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39). • "ICT readiness for business continuity" (27K1:2022 A.5.30). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices and physical security management are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers' content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data according their own business continuity and disaster recovery strategies; if available, additional georedundancy services can be enabled. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/. To learn more about Acronis' data center security posture, please refer to https://www.acronis.com/resource-center/resource/acronis-cloud-data-centers-a-primer-on-security-privacy-and-compliance/.
2.5. Restrictions on Bringing Personal Belongings.	❶ Restrictions on bringing personal belongings into facilities where medical information is processed.	❶-1	Restrict the bringing of personal belongings unrelated to the execution of duties into medical information processing facilities.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). • "Security of equipment and assets off-premises" (27K1:2013 A.11.2.6; 27K1:2022 A.7.9). • "Acceptable use of the assets" (27K1:2013 A.8.1.3; 27K1:2022 A.5.10). Acronis' employees do not have access to customers' content data. Customers' content data is not exported for any reason on Acronis employees' terminals. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-2	Restrict the bringing of personal belongings unrelated to the execution of duties into locations where devices and media are installed.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
2.6. Measures Against Equipment Theft.	❶ Attachment of anti-theft chains or similar devices to important equipment.	❶-1	Attach theft prevention chains or similar devices to important equipment, such as PCs that contain personal information.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Physical and environmental security” (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). • “Security of equipment and assets off-premises” (27K1:2013 A.11.2.6; 27K1:2022 A.7.9). • “Acceptable use of the assets” (27K1:2013 A.8.1.3; 27K1:2022 A.5.10). Acronis’ employees do not have access to customers’ content data. Customers’ content data is not exported for any reason on Acronis employees’ terminals. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
2.7. Measures Against Snooping.	❶ Measures to Prevent Snooping.	❶-1	Take measures, such as adjusting the layout of devices within the room, to ensure that terminal screens displaying medical information, etc., are not within the field of view of those without access rights.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Physical and environmental security” (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). • “Security of equipment and assets off-premises” (27K1:2013 A.11.2.6; 27K1:2022 A.7.9). • “Acceptable use of the assets” (27K1:2013 A.8.1.3; 27K1:2022 A.5.10). Acronis’ employees do not have access to customers’ content data. Customers’ content data is not exported for any reason on Acronis employees’ terminals. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-2	To prevent snooping while personal information is displayed, implement measures such as applying privacy filters to terminals.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
2.8. Measures Against Disasters.	❶ Measures against earthquakes, floods, lightning, fires, and related power outages.	❶-1	Facilities used for the physical storage of devices and media should be equipped with functions and structures that can withstand disasters (such as earthquakes, floods, lightning, fires, and related power outages), and be located in buildings where measures have been taken to address issues caused by disasters, such as condensation.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Physical and environmental security” (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6) Physical security for colocated data centers is responsibility shared with each data center facility. Acronis has established partnerships that run numerous global, colocated data center facilities. These facilities meet rigorous standards and compliance needs regarding setup, power and cooling. This approach maintains optimal conditions and uptime to safeguard mission-critical data. Additionally, Acronis has strict requirements for data center locations to reduce or eliminate the probability of the most typical disruptive events. During the term of each contract, Acronis regularly monitors and reviews the third party’s security controls, service delivery and compliance with contractual requirements. Information security oversight and management controls, including physical security management practices are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. To learn more about Acronis’ data center security posture, please refer to https://www.acronis.com/resource-center/resource/acronis-cloud-data-centers-a-primer-on-security-privacy-and-compliance/.
		❶-2	Agree with medical institutions, etc., regarding the buildings in which the facilities mentioned in ❶-1 are installed.	
		❶-3	Take care to ensure that firefighting equipment does not damage the equipment in the event of a fire.	
		❶-4	Prohibit smoking and eating in rooms where medical information systems, etc., are located.	
		❶-5	When placing combustible materials and liquids in rooms where medical information systems, etc., are located, ensure a sufficient distance from the equipment and consider providing dedicated storage facilities to prevent adverse effects on the equipment.	
		❶-6	Implement the following safety management measures for server racks where medical information systems, etc., are installed: • Ensure stable installation to prevent tipping over in the event of an earthquake. • Maintain adequate air conditioning facilities to prevent heat-related issues and ensure sufficient ventilation within the server racks. • Equip doors with physical locking devices of sufficient safety strength and give careful consideration to key management.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3. Technical Measures				
3.1. Implementation of User Authentication.	❶ Adoption of methods for uniquely identifying users.	❶-1	When registering, editing, or deleting information in medical information systems, etc., design and implement a system that requires users to log on in order to identify them and verify their permissions.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis keeps strict segregation of duties and grants privileged access on role base. Acronis' employees do not have access to customers' content data. Customers' content data is not exported for any reason on Acronis employees' terminals. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.
		❶-2	Issue accounts to identify and distinguish users of medical information systems, etc. (Do not allow multiple users to share an ID. However, IDs used by the medical information system, etc., to access other medical information systems, known as non-interactive IDs, are excluded).	
		❶-3	Implement authentication to prevent impersonation and similar issues among users.	
		❶-4	Issue IDs to individuals involved in the operation or development of medical information systems, etc., or those with administrative privileges, to the minimum necessary extent and conduct regular audits.	
	❷ Preparation of temporary authentication methods.	❷-1	When user authentication requires some form of physical media or biometric information, establish in advance alternative means or procedures for temporary authentication in exceptional cases where those media are unavailable.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis keeps strict segregation of duties and grants privileged access on role base via zero trust infrastructure with mandatory multifactor authentication methods. Acronis Cyber Protect Cloud offer to its users to set up a multifactor authentication, is customers responsibilities enable it according to their needs. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.
		❷-2	In cases where alternative means or procedures are used, minimize the risk difference compared to when the original user authentication method is employed.	
		❷-3	Even when access to medical information systems is granted through alternative means or procedures, keep records that enable post-hoc tracking and manage these records.	
		❷-4	Agree with medical institutions on other temporary user authentication methods.	
	❸ Measures for Extended Absences from the Workstation.	❸-1	Lock the terminal or log off when leaving the desk or not using it, to prevent unauthorized use by third parties in advance.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Unattended user equipment" (27K1:2013 A.11.2.8; 27K1:2022 A.8.1). • "Data leakage prevention" (27K1:2022 8.12). Acronis has established specific policies and procedures regarding the acceptable use of assets, requiring employees to keep their desks and screens free of sensitive data and to lock their terminals when unattended. Technical measures are implemented to block users' machines after a specified period of inactivity.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❸-2	Specify in the operational management policies and related documents the implementation of preventive measures such as clear screen policies for service operation and maintenance terminals, etc.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Clear desk and clear screen policy" (27K1:2013 A.11.2.9; 27K1:2022 A.7.7). • "Data leakage prevention" (27K1:2022 8.12).
		❸-3	Agree with medical institutions, etc., on information leakage prevention measures such as clear screen policies for user terminals, etc., that can access and reference medical information installed at medical institutions.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Clear desk and clear screen policy" (27K1:2013 A.11.2.9; 27K1:2022 A.7.7). • "Data leakage prevention" (27K1:2022 8.12). Acronis' employees do not have access to customers' content data. Customers' content data is not exported for any reason on Acronis employees' terminals. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including development of operational procedures and guidelines.
		❸-4	To reduce the risk of terminal or session hijacking, disrupt the session or enforce a logoff after a certain period of inactivity following user logon.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Unattended user equipment" (27K1:2013 A.11.2.8; 27K1:2022 A.8.1). • "Data leakage prevention" (27K1:2022 8.12).
		❸-5	Agree with medical institutions, etc., on the specific application of close procedures in case of absence.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Unattended user equipment" (27K1:2013 A.11.2.8; 27K1:2022 A.8.1). • "Data leakage prevention" (27K1:2022 8.12). Acronis has implemented session locks on end-user computers, in the form of a password-protected screensaver, triggered after 15 minutes of inactivity. This screensaver remains locked until the user signs back into their computer. Additionally, Acronis enforces encrypted sessions for connections to the production environment, effectively thwarting any attempts at man-in-the-middle attacks or hijacking of idle sessions.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	4 Definition of Secure Password Requirements.	4-1	Establish quality standards for passwords that include content not easily guessed by third parties, and ensure that all passwords meet these quality standards.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Password management system" (27K1:2013 A.9.4.3; 27K1:2022 A.5.17). • "Access control" (27K1:2013 A.9.1; 27K1:2022 A.5.15). • "Identity management (27K1:2013 A.9.2.1; 27K1:2022 A.5.16). • "Authentication Information" (27K1:2013 A.9.2.4, A.9.3.1, A.9.4.3; 27K1:2022 A.5.17). • "Access right" (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). • "Secure authentication" (27K1:2013 A.9.4.2; 27K1:2022 A.8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis keeps strict segregation of duties and grants privileged access on role base via zero trust infrastructure with mandatory multifactor authentication methods. Acronis employee password are regularly audited with automatic tool to discover weak or leaked passwords. Acronis Cyber Protect Cloud offer to its users to set up a multifactor authentication, is customers responsibilities enable it according to their needs. Threat intelligence system is running to find evidence of leaked Acronis customer passwords. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.
		4-2	Agree with medical institutions on the password policy.	
		4-3	Set expiration dates for passwords and enforce their regular change. However, when users are patients, etc., not only strongly encourage them not to use passwords utilized for other services, but also ensure that the service provider does not require patients to regularly change their passwords.	
		4-4	Implement password generation management and operate in such a way that, to ensure security, passwords previously set cannot be reused when changing passwords, within the necessary scope.	
		4-5	Issue temporary login passwords for medical information systems, etc., generated from random numbers at the time of password issuance, and implement measures against password theft risk, such as mandating a change at the first login.	
		4-6	Ensure workers do not use the automatic logon function to store passwords in the system.	
		4-7	When users register or change their passwords, implement mechanisms to ensure the passwords meet predefined quality standards, such as introducing programs that generate passwords using random numbers and adopting systems that do not allow the setting of low-quality passwords.	
		4-8	Take measures to ensure that information used for personal identification and authentication is kept in a state that only the individual concerned can know.	
		4-9	When issuing initial passwords to users, ensure that they must change the password upon first use before they can access the medical information system, etc.	
		4-10	Require that passwords, other than the initial password, are set by the users themselves and that the content of these passwords is known only to the user.	
		4-11	When setting passwords, use a rule that includes a mix of character types (alphabetic, uppercase, lowercase, symbols, etc.) and is of a sufficiently safe length, such as at least 8 characters.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		4-12	When users forget their ID or password, notify them or reissue it according to previously established procedures, including verification of identity.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Password management system” (27K1:2013 A.9.4.3; 27K1:2022 A.5.17). • “Access control” (27K1:2013 A.9.1; 27K1:2022 A.5.15). • “Identity management (27K1:2013 A.9.2.1; 27K1:2022 A.5.16). • “Authentication Information” (27K1:2013 A.9.2.4, A.9.3.1, A.9.4.3; 27K1:2022 A.5.17). • “Access right” (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). • “Secure authentication” (27K1:2013 A.9.4.2; 27K1:2022 A.8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis keeps strict segregation of duties and grants privileged access on role base via zero trust infrastructure with mandatory multifactor authentication methods. Acronis employee password are regularly audited with automatic tool to discover weak or leaked passwords. Acronis Cyber Protect Cloud offer to its users to set up a multifactor authentication, is customers responsibilities enable it according to their needs. Threat intelligence system is running to find evidence of leaked Acronis customer passwords. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.
		4-13	Require the input of the previous password when changing passwords, and if the input of the previous password fails a certain number of times, implement a mechanism to not accept password changes for a specified period.	
		4-14	Set a specific delay period for re-entering the password after an unsuccessful attempt. If logon attempts fail consecutively, implement a mechanism to not accept re-entry for a certain period. In such cases, introduce a system to send a warning message to the system administrator.	
	5 Adoption of Multi-Factor Authentication Methods.	5-1	It is desirable to use multi-factor authentication at logon, combining authentication devices such as hardware tokens or IC cards, memorized elements like PINs or passwords, and biometric information (biometrics).	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Password management system” (27K1:2013 A.9.4.3; 27K1:2022 A.5.17). • “Access control” (27K1:2013 A.9.1; 27K1:2022 A.5.15). • “Identity management (27K1:2013 A.9.2.1; 27K1:2022 A.5.16). • “Authentication Information” (27K1:2013 A.9.2.4, A.9.3.1, A.9.4.3; 27K1:2022 A.5.17). • “Access right” (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). • “Secure authentication” (27K1:2013 A.9.4.2; 27K1:2022 A.8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis keeps strict segregation of duties and grants privileged access on role base via zero trust infrastructure with mandatory multifactor authentication methods. Acronis Cyber Protect Cloud offer to its users to set up a multifactor authentication, is customers responsibilities enable it according to their needs. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.
		5-2	Authentication related to the use of information systems by those engaged in the operation or development of medical information systems, etc., or those with administrative privileges, should be multi-factor authentication.	
		5-3	Agree with medical institutions, etc., on the authentication methods to be used for user authentication.	
		5-4	When adopting an authentication method based on ID and password for user authentication, strive to equip the system with capabilities that can support authentication methods not solely reliant on ID and password. Notably, in the guidelines for the security management of medical information systems, it is stated that approximately 10 years after the publication of the 5th edition of the guidelines (May 2017), moving towards two-factor authentication is anticipated as a minimum guideline in the Ministry of Health, Labour and Welfare’s guidelines, section 6.5 ‘C. Minimum Guidelines.’ Therefore, ensure the system can adapt to this guideline in a timely manner.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.2 Access Rights Management.	❶ Management of access rights to ensure they are limited to the minimum necessary.	❶-1	Enable access management for the operation of medical information systems in accordance with the job authority of medical institutions to prevent the creation, viewing, editing, and deletion of information by those who do not have legitimate access rights.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Password management system" (27K1:2013 A.9.4.3; 27K1:2022 A.5.17). • "Access control" (27K1:2013 A.9.1; 27K1:2022 A.5.15). • "Identity management (27K1:2013 A.9.2.1; 27K1:2022 A.5.16). • "Authentication Information" (27K1:2013 A.9.2.4, A.9.3.1, A.9.4.3; 27K1:2022 A.5.17). • "Access right" (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). • "Secure authentication" (27K1:2013 A.9.4.2; 27K1:2022 A.8.5). • "Independent review of information security" (27K1:2013 A.18.2.1; 27K1:2022 A.5.35). • "Classification of information" (27K1:2013 A.8.2.1; 27K1:2022 A.5.12). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis keeps strict segregation of duties and grants privileged access on role base via zero trust infrastructure with mandatory multifactor authentication methods. Acronis Cyber Protect Cloud allows its users to set up multifactor authentication; but it's the customer's responsibility to enable it according to their needs. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.
		❶-2	Present the settings for access control based on the job types of users at medical institutions conduct the necessary consultations with them, and agree on the division of responsibilities for the actual setting work.	
		❶-3	Organize the security requirements related to access management for each component of medical information systems, etc. (information processing equipment, software).	
		❶-4	Appropriately group information to minimize the number of users who have access rights to each piece of information, and implement access control for these groups of information.	
		❶-5	Establish the minimum necessary access rights considering the nature of the work, and set permissions in applications and operating systems.	
		❶-6	It is essential to conduct regular audits to ensure that established access control policies are effectively implemented through mechanisms such as file and directory permissions and database access.	
		❶-7	To prevent unauthorized viewing of entrusted medical information during scheduled maintenance and operations, implement measures such as setting permissions.	
		❶-8	Implement measures (such as database encryption) to ensure that system administrators, operators, and maintenance personnel do not inadvertently access data.	
	❷ Access Control for Medical Information.	❷-1	Implement measures to distinguish between medical information and other types of information.	Not applicable. This is the customer's responsibility to respond to.
		❷-2	Ensure that access control for medical information is conducted in accordance with information classification.	Not applicable. This is the customer's responsibility to respond to.
		❷-3	When providing resources using virtualization technology, implement measures to ensure that logical segregation management can be performed.	Not applicable. This is the customer's responsibility to respond to.
		❷-4	Agree with medical institutions, etc., on setting classifications for information assets and configuring access controls for these classifications.	Not applicable. This is the customer's responsibility to respond to.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.3 Management of IDs and Passwords.	❶ User Access and Management/ Operation of IDs.	❶-1	Identify users on medical information systems with a unique ID for each user.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Password management system" (27K1:2013 A.9.4.3; 27K1:2022 A.5.17). • "Access control" (27K1:2013 A.9.1; 27K1:2022 A.5.15). • "Identity management (27K1:2013 A.9.2.1; 27K1:2022 A.5.16). • "Authentication Information" (27K1:2013 A.9.2.4, A.9.3.1, A.9.4.3; 27K1:2022 A.5.17). • "Access right" (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). • "Secure authentication" (27K1:2013 A.9.4.2; 27K1:2022 A.8.5). • "Independent review of information security" (27K1:2013 A.18.2.1; 27K1:2022 A.5.35). • "Classification of information" (27K1:2013 A.8.2.1; 27K1:2022 A.5.12). • "Logging" (27K1:2013 A.12.4; 27K1:2022 A.8.15). • "Monitoring activities" (27K1:2022 A.8.16). • "Use of privileged utility programs" (27K1:2013 A.9.4.4; 27K1:2022 A.8.18). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis keeps strict segregation of duties and grants privileged access on role base via zero trust infrastructure with mandatory multifactor authentication methods. Acronis Cyber Protect Cloud allows its users to set up multifactor authentication; but it's the customer's responsibility to enable it according to their needs. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.
		❶-2	Implement a system to eliminate duplication with existing IDs when issuing user IDs.	
		❶-3	As a principle, do not use group IDs shared by multiple users. If necessary for business purposes, use a system where users log on with their individual IDs and then switch to a group ID, ensuring that the executor of operations can be identified in the logs.	
		❶-4	Limit the issuance of user IDs to the minimum number of people necessary for the management of medical information systems.	
		❶-5	To ensure accurate identification of users during the audit of monitoring logs, do not reuse past user IDs.	
		❶-6	It is recommended to regularly verify that the access range available through the IDs of authorized users is as permitted (and has not been altered unauthorizedly).	
		❶-7	To enable users to detect unauthorized account usage or attempts themselves, display the date and time of the last successful login after a user logs on, if the last login attempt was successful.	
		❶-8	To prevent unauthorized account use, it is advisable to restrict the days and times users are allowed to log on to those necessary for their work.	
		❶-9	To avoid giving clues that a particular ID exists when unauthorized users or third parties attempt to log on, it is preferable to limit the message to a non-specific expression such as 'Authentication failed' or simply redisplaying the login prompt, rather than stating 'The password is incorrect'.	
		❶-10	It is recommended to develop a reasonable approval process for logging on outside of regular hours in case of emergency work needs.	
		❶-11	When there is suspicion of unauthorized access to medical information systems, etc., or the possibility that a password has been disclosed to a third party, immediately change the password or disable the account and notify the administrator.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-12	When a user changes or retires, the user ID must be disabled immediately.	
		❶-13	Regularly verify that there are no unnecessary user IDs remaining.	
	❷ Minimal use of privileged IDs and recording of performed activities.	❷-1	Limit the issuance of privileged IDs to the minimum necessary.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Password management system" (27K1:2013 A.9.4.3; 27K1:2022 A.5.17). • "Access control" (27K1:2013 A.9.1; 27K1:2022 A.5.15). • "Identity management (27K1:2013 A.9.2.1; 27K1:2022 A.5.16). • "Authentication Information" (27K1:2013 A.9.2.4, A.9.3.1, A.9.4.3; 27K1:2022 A.5.17). • "Access right" (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). • "Secure authentication" (27K1:2013 A.9.4.2; 27K1:2022 A.8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis keeps strict segregation of duties and grants privileged access on role base via zero trust infrastructure with mandatory multifactor authentication methods. Acronis Cyber Protect Cloud allows its users to set up multifactor authentication; but it's the customer's responsibility to enable it according to their needs. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.
		❷-2	Restrict user IDs that can be elevated to privileged users.	
		❷-3	Record the activities' details performed when using privileges.	
		❷-4	Prohibit direct logon with privileged IDs from non-administrative terminals.	
		❷-5	It is recommended to segregate accounts according to the type of privilege and restrict access to files and directories accordingly.	
		❷-6	If possible as a function of medical information systems it is recommended to restrict the commands and utilities available to privileged IDs to the minimum necessary for business purposes. It is also desirable to prevent unauthorized actions such as tampering or deletion regarding important commands, utilities, and logs.	
	❸ Management and Operation of Passwords.	❸-1	Each user must keep their password confidential. If there is a need to record the password, it should be stored in a secure location to protect it from unauthorized access, modification, or disposal by others.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Password management system" (27K1:2013 A.9.4.3; 27K1:2022 A.5.17). • "Access control" (27K1:2013 A.9.1; 27K1:2022 A.5.15). • "Identity management (27K1:2013 A.9.2.1; 27K1:2022 A.5.16). • "Authentication Information" (27K1:2013 A.9.2.4, A.9.3.1, A.9.4.3; 27K1:2022 A.5.17). • "Access right" (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). • "Secure authentication" (27K1:2013 A.9.4.2; 27K1:2022 A.8.5). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis keeps strict segregation of duties and grant privileged access on role base via zero trust infrastructure with mandatory multifactor authentication methods. Acronis Cyber Protect Cloud allows its users to set up multifactor authentication; but it's the customer's responsibility to enable it according to their needs. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❸-2	Before using medical information systems and software, conduct an inventory of default accounts and maintenance accounts set by the manufacturer. Disable any unnecessary accounts.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Configuration management” (27K1:2022 A.8.9). • “Networks Security” (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report.
		❸-3	Store passwords in a form that cannot be easily restored, such as by saving as hash values or through encryption.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Password management system” (27K1:2013 A.9.4.3; 27K1:2022 A.5.17). • “Use of cryptography” (27K1:2013 A.10.1; 27K1:2022 A.8.24). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report.
		❸-4	To maintain the authenticity and integrity of files storing password-related data, adopt protective measures such as obtaining and verifying file hash values, applying and verifying digital signatures on files, and encrypting files for storage. Additionally, restrict access to these files from general users.	
		❸-5	In the event of a leakage of information such as passwords (including cases due to unauthorized attacks by third parties), immediately disable the relevant ID. Based on previously established procedures, reissue new login information and promptly notify the user.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • “Information security incident management planning and preparation” (27K1:2013 A.16.1.1; 27K1:2022 A.5.24). • “Assessments and decisions on information security events” (27K1:2013 A.16.1.4; 27K1:2022 A.5.25). • “Response to information security incidents” (27K1:2013 A16.1.5; 27K1:2022 A.5.26). • “Reporting information security events” (27K1:2013 A.16.1.2; 27K1:2022 A.6.8). Acronis maintains a stringent incident management process dedicated to addressing security incidents that may compromise the confidentiality, integrity or availability of its systems or data. When a security incident is identified, the Acronis security team promptly logs and categorizes the incident according to its severity. Incidents affecting customers directly are given the highest priority. The process details specific actions, notification and escalation procedures, mitigation steps and documentation practices. Regular testing of the incident response plans is conducted, with a special focus on systems containing sensitive customer data. These tests cover various threat scenarios, including internal risks and software vulnerabilities, to ensure the team’s readiness. In cases where a security breach involves customer data, Acronis and its partners commit to promptly notifying the affected customers and offering comprehensive support through the investigation process. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment, so as detect unauthorized access and take actions to mitigate it eventually.
		❸-6	In cases where there is a risk of password or similar information leakage, notify the user of the fact, then disable the password in question, and take measures to enable its change.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.4. Log Acquisition and Verification.	❶ Acquisition and Verification of Logs.	❶-1	Create logs that record user activities, events occurring on devices, system failures, system usage and retain these logs for a specified period.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Logging” (27K1:2013 A.12.4; 27K1:2022 A.8.15). • “Monitoring activities“ (27K1:2022 A.8.16). Information security oversight and management controls, including logical access controls, logging and monitoring activities are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis continuously monitors audit logs through its proprietary Security Information and Event Management system to identify intrusion attempts and other security-related events. Security alerts are generated for further investigation based on predefined thresholds. These monitoring tools automatically issue alerts to security personnel. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment, including log management and monitoring activities.
		❶-2	Regularly verify logs to detect unauthorized activities, system anomalies, etc.	
		❶-3	Items to be recorded in logs could include the following: • User information (user ID, logon success or failure, usage time and duration, tasks performed, source IP address in case of network access) • Access, modification, and deletion records for files and data (user ID, access granted or denied, usage time and duration, nature of the task, targeted file or data type) • Database operation records (user ID, connection and operation success or failure, usage time and duration, tasks performed, source IP address, and details of configuration changes) • Patch application activities (user ID, files changed) • Privileged operations (privileged user ID, privilege acquisition success or failure, usage time and duration, tasks performed) • System start-up and shut-down events • Start and end events of log acquisition functionality • External device removal • Security device event logs such as IDS/IPS Logs generated by service and application activities (including logs related to time synchronization)	
		❶-4	If possible, log data will be aggregated, analyzed and managed on a dedicated log server for the purpose of centralizing logs and reliably detecting problems in one place.	
		❶-5	Acquire necessary logs for auditing when updating library programs related to operational systems.	
		❶-6	Acquire logs for audit trails when duplicating and using system operational information (such as system and service configuration files).	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-7	Regularly review the records of access by those engaged in the operation or development of medical information systems or those with administrative privileges, to confirm that there has been no unauthorized access or similar issues.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access control" (27K1:2013 A.9.1; 27K1:2022 A.5.15). • "Logging" (27K1:2013 A.12.4; 27K1:2022 A.8.15). • "Monitoring activities" (27K1:2022 A.8.16). Information security oversight and management controls, including logical access controls, logging and monitoring activities are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis continuously monitors audit logs through its proprietary Security Information and Event Management system to identify intrusion attempts and other security-related events. Security alerts are generated for further investigation based on predefined thresholds. These monitoring tools automatically issue alerts to security personnel. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment, including access management and monitoring activities.
		❶-8	Agree with medical institutions on the provision of information on ❶-7.	
		❶-9	Agree with the medical institution, in case of not having functions to acquire logs.	Acronis Cyber Protect Cloud provides advanced XDR functions and integration with several SIEM systems.
		❶-10	Individuals engaged in the maintenance of medical information systems and those with administrative privileges should access these systems using accounts issued to each personnel for the purpose of their duties.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access control" (27K1:2013 A.9.1; 27K1:2022 A.5.15). • "Logging" (27K1:2013 A.12.4; 27K1:2022 A.8.15). • "Monitoring activities" (27K1:2022 A.8.16). • "Access right" (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). • "Use of privileged utility programs" (27K1:2013 A.9.4.4; 27K1:2022 A.8.18). Information security oversight and management controls, including logical access controls, logging and monitoring activities are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis continuously monitors audit logs through its proprietary Security Information and Event Management system to identify intrusion attempts and other security-related events. Security alerts are generated for further investigation based on predefined thresholds. These monitoring tools automatically issue alerts to security personnel. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment, including access management and monitoring activities.
		❶-11	Work performed using the accounts specified in ❶-10 should be recorded and saved in logs or similar means in a manner that allows for the identification of accessed personal information.	
		❶-12	Record and manage the results of operations performed during the maintenance of medical information systems using operation logs or similar means.	
		❶-13	Review the situation of the medical information accessed, using the acquired operation logs or similar means.	
		❶-14	To facilitate the verification of logs, it is advisable to maintain a system that allows for the quick confirmation of medical information accessed by users. This system should enable sorting and filtering based on various criteria such as the user's ID, the identifier of the information (e.g., numbers listed in the asset register), chronological order of creation, access sequence, type of information, access time, and more.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	❷ Access restrictions and external storage to prevent tampering or deletion of logs.	❷-1	To appropriately protect log information from unauthorized access, apply the following management strategies: · Restrict users and operations that can access log data. · Constantly monitor the storage capacity of the log server to avoid situations where logs cannot be captured due to capacity overload, and take measures such as exporting to electronic media and increasing capacity. · Implement detection and prevention measures against unauthorized tampering and deletion of log data.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: · “Access control” (27K1:2013 A.9.1; 27K1:2022 A.5.15). · “Logging” (27K1:2013 A.12.4; 27K1:2022 A.8.15). · “Monitoring activities“ (27K1:2022 A.8.16). · “Access right” (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). · “Use of privileged utility programs” (27K1:2013 A.9.4.4; 27K1:2022 A.8.18). Information security oversight and management controls, including logical access controls, logging and monitoring activities are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis continuously monitors audit logs through its proprietary Security Information and Event Management system to identify intrusion attempts and other security-related events. Security alerts are generated for further investigation based on predefined thresholds. These monitoring tools automatically issue alerts to security personnel. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment, including access management and monitoring activities.
	❸ Synchronization the clock to Standard Time.	❸-1	To accurately verify the cause of incidents using logs, synchronize the clocks of all server equipment in medical information systems, etc., with the standard time provided by a time server or similar.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: · “Clock synchronization” (27K1:2013 A.12.4.4; 27K1:2022 A.8.17).
		❸-2	It is recommended to regularly verify that the clocks of all server equipment in medical information systems, etc., are synchronized with the standard time provided by a time server or similar.	
		❸-3	To ensure the reliability of log timestamps, synchronize the clocks of medical information systems with the standard time provided by a trusted authority or equivalent time information daily or at a higher frequency.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	❹ Preventing Unauthorized Intrusion in Remote Maintenance and Acquisition and Verification of Logs.	❹-1	Develop procedures for conducting maintenance work via remote maintenance, and take safety management measures to prevent unauthorized intrusion into medical information systems.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Access control” (27K1:2013 A.9.1; 27K1:2022 A.5.15). • “Logging” (27K1:2013 A.12.4; 27K1:2022 A.8.15). • “Monitoring activities“ (27K1:2022 A.8.16). • “Access right” (27K1:2013 A.9.2.2, A.9.2.5, A.9.2.6; 27K1:2022 A.5.18). • “Use of privileged utility programs” (27K1:2013 A.9.4.4; 27K1:2022 A.8.18). Information security oversight and management controls, including logical access controls, logging and monitoring activities are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis continuously monitors audit logs through its proprietary Security Information and Event Management system to identify intrusion attempts and other security-related events. Security alerts are generated for further investigation based on predefined thresholds. These monitoring tools automatically issue alerts to security personnel. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment, including access management and monitoring activities.
		❹-2	Acquire records of maintenance work performed through remote maintenance using access logs and similar methods, and ensure that system administrators promptly verify the contents.	
		❹-3	When performing remote maintenance of medical information systems necessary for service provision, agree with medical institutions.	
	❺ Setting the retention period for logs based on the legal retention period of the medical information handled.	❺-1	If there is a legal retention period set for the medical information handled, establish a retention period for logs related to medical records or equivalent records that is at least as long as the legal requirement.	Not applicable. This is the customer’s responsibility to respond to.
		❺-2	Agree with medical institutions on the retention period for medical information after the legal retention period has elapsed and for medical information that does not have a designated legal retention period. If a retention period for the management method of logs is established in this section, it should, as a principle, be handled in accordance with the medical information that has a legal retention period.	Not applicable. This is the customer’s responsibility to respond to.
3.5. Measures Against Malicious Programs.	❶ Installation and Management of anti-malware software.	❶-1	Make efforts to collect information on the latest threats, verify the coverage of the anti-malware software that has been introduced, and ensure there are no gaps in protection. Examples of threats that should be addressed include computer viruses (worms), backdoors (Trojans), spyware (keyloggers), and bot programs (downloaders).	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • “Protection against malware” (27K1:2013 A.12.2.1; 27K1:2022 A.8.7). • “Information security incident management planning and preparation” (27K1:2013 A.16.1.1; 27K1:2022 A.5.24). • “Assessments and decisions on information security events” (27K1:2013 A.16.1.4; 27K1:2022 A.5.25). • “Response to information security incidents” (27K1:2013 A16.1.5; 27K1:2022 A.5.26). “Reporting information security events” (27K1:2013 A.16.1.2; 27K1:2022 A.6.8). Acronis uses its own developed product to handle malware threats and assure protection at the endpoint level. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-2	In the anti-malware software, make the following settings: • Real-time scanning (disk writing and reading, network communication) • Periodically scan if necessary as a result of risk assessment. • On-demand scan files when writing and reading data to and from electronic media.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-3	If a device has not undergone a check for malicious programs for a specified period, or if the definition files or scan engine have not been updated, take actions such as displaying a warning to the user, notifying the administrator, and prohibiting or isolating the device from the facility's network.	
		❶-4	When constructing medical information systems, develop procedures to prevent the infiltration of malicious programs and build according to these procedures.	
		❶-5	Always update the pattern definition files of the anti-malware software to the latest version.	
		❶-6	"When constructing medical information systems if it is necessary to bring in or download programs from external sources, always ensure the latest anti-malware software is installed in advance. Also, considering the impact on the information system, apply the latest security patches.	
		❶-7	In the event that the environment using medical information systems, etc., is attacked by viruses or similar threats, promptly inform medical institutions, etc., about the impact on the provision of medical information systems and request necessary actions.	
3.6. Hardening of Terminals and Servers.	❶ Hardening of Terminals and Servers.	❶-1	Store medical information only on server equipment, ensuring it is not saved on terminals except for temporary storage needed for display purposes.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). Information security oversight and management controls, including logical access controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis keeps strict segregation of duties and grants privileged access on role base. Acronis' employees do not have access to customers' content data. Customers' content data is not exported for any reason on Acronis employees' terminals. Acronis storage is encrypted at rest by AES-256. Depending on the product used, customers can also enable encryption from their side before sending data to Acronis Cyber Cloud Storage. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including access management and data encryption, according to their own needs.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-2	Restrict web browser connections to only those servers necessary for business purposes.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • "Protection against malware" (27K1:2013 A.12.2.1; 27K1:2022 A.8.7). • "Web filtering" (27K1:2022 A.8.23). Acronis uses its own developed product to handle malware threats and assure protection at the end point level. Web filtering is enabled on end users' devices, blocking suspicious IPs and URLs according threat intelligence results. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-3	In web browser settings, configure to prevent the download and execution of program codes such as ActiveX, Java applets, Flash, etc., from unauthorized sites (only authorize servers where management software is executed).	
		❶-4	Inspect code downloaded from authorized sites with anti-malware software as well.	
		❶-5	It is recommended to configure settings so that external applications not anticipated in business processes, such as email clients, are not launched from the web browser without explicit confirmation.	
		❶-6	Set an appropriate upper limit on the number of concurrent logon users (such as OS accounts) to medical information systems and server equipment.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2).
		❶-7	Do not install unnecessary applications on devices used for medical information systems.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Responsibility for assets" (27K1:2022 A.8.1; 27K1:2022 A.5.9, A.5.10, A.5.11). • "Disposal of Media" (27K1:2013 A.8.3.2; 27K1:2022 A.7.10). • "Secure disposal or reuse of equipment" (27K1:2013 A.11.2.7; 27K1:2022 A.14). • "Installation of software on operational systems" (ISO27K1:2013 A.12.5.1, A.12.6.2; ISO27K1:2022 A.8.19).
		❶-8	When removing devices that store information related to medical information systems install only the minimum necessary applications required for the purpose of the removal.	
		❶-9	Establish procedures for installing applications when removing devices that store information related to medical information systems.	
3.7. Addressing Vulnerabilities in Devices and Software.	❶ Use of network devices whose safety has been verified.	❶-1	Use network devices such as routers whose safety has been confirmed.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Managing information in the ICT supply chain" (27K1:2013 A.15.1.3; 27K1:2022 A.5.21). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). • "Responsibility for assets" (27K1:2022 A.8.1; 27K1:2022 A.5.9, A.5.10, A.5.11). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-2	Select network devices such as routers that have a Security Target or similar document specified by ISO/IEC 15408, which conforms to this guideline.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	② Implementation of Patch Application.	②-1	Manage technical vulnerabilities related to medical information systems using a ledger or similar tool.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Management of technical vulnerabilities" (27K1:2013 A.12.6.1, A.18.2.3; 27K1:2022 A.8.8). • "Change management" (27K1:2013 A.12.1.2; 27K1:2022 A.8.32). • "System acquisition, development and maintenance" (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). Acronis implements a comprehensive vulnerability management program that proactively identifies security threats through a blend of market-available and custom-developed in-house tools, alongside rigorous automated and manual penetration testing, quality assurance measures, software security assessments and external audits. The responsibility for monitoring and addressing vulnerabilities lies with Acronis' cybersecurity team, which meticulously identifies and tracks these issues, ensuring regular follow ups until remediation is confirmed. Furthermore, Acronis cultivates strong connections with independent security researchers running a bug bounty program. Controls relating to vulnerability management and change management are also reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. More information on Acronis' cybersecurity posture can be found at https://www.acronis.com/trust-center/.
		②-2	When potential technical vulnerabilities are identified, conduct a risk analysis and then decide on the necessary measures (such as applying patches or changing settings).	
		②-3	Before applying a patch, verify that the patch has not been tampered with and validate its effectiveness.	
		②-4	When upgrading the operating system or applying security patches, evaluate the impact on medical information systems and proceed with the implementation after confirming the test results.	
	③ Conducting Vulnerability Assessments on Medical Information Systems.	③-1	Regularly conduct security assessments on the applications provided, including the detection of vulnerabilities specific to the type of application, and take measures based on the results. Implement a mechanism to verify the integrity of data when exchanging data with medical institutions.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Management of technical vulnerabilities" (27K1:2013 A.12.6.1, A.18.2.3; 27K1:2022 A.8.8). • "System acquisition, development and maintenance" (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). Acronis implements a comprehensive vulnerability management program that proactively identifies security threats through a blend of market-available and custom-developed in-house tools, alongside rigorous automated and manual penetration testing, quality assurance measures, software security assessments and external audits. The responsibility for monitoring and addressing vulnerabilities lies with Acronis' cybersecurity team, which meticulously identifies and tracks these issues, ensuring regular follow up until remediation is confirmed. A Security Development Life Cycle (SDLC) has been established to assure multiple software security checks from the design to the deployment. A bug bounty program is run to involve independent security researchers. Controls relating to vulnerability management are also reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. More information on Acronis' cybersecurity posture can be found at https://www.acronis.com/trust-center/.
		③-2	It is recommended to conduct security assessments of applications not directly on the services provided, but rather in a separate testing environment.	
		③-3	It is recommended to conduct vulnerability detection of developed software at the source code level. For packaged software and other instances where source code cannot be requested, perform external vulnerability testing by operating the application, rather than at the source code level.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
	❹ Information Gathering on the Latest Vulnerabilities.	❹-1	For applications and third-party software used in the operation of applications (libraries, server processes, etc.), refer to the latest published vulnerability information and take prompt corrective action.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Managing information in the ICT supply chain" (27K1:2013 A.15.1.3; 27K1:2022 A.5.21). • "Management of technical vulnerabilities" (27K1:2013 A.12.6.1, A.18.2.3; 27K1:2022 A.8.8). • "System acquisition, development and maintenance" (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❹-2	Regularly and as necessary, obtain and verify information on vulnerabilities in medical information systems from sources such as the JPCERT Coordination Center (JPCERT/CC), the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), and the Information-technology Promotion Agency (IPA).	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Threat intelligence" (27K1:2022 A.5.7).
	❺ Information Gathering and Response to Vulnerabilities in IoT Devices.	❺-1	When providing services that include the use of IoT devices, agree with medical institutions on the division of roles and responsibilities.	Not applicable. This is the customer's responsibility to respond to.
		❺-2	When providing services that include the use of IoT devices, agree with medical institutions on the division of roles and responsibilities.	Not applicable. This is the customer's responsibility to respond to.
3.8. Network Access Control.	❶ Control of Network Access.	❶-1	Install security gateways (firewalls, routers, etc., placed at the network boundary) to perform access control on each network interface based on established policies, such as limiting connection destinations and connection times. When using hosting services or in cases where it is not possible to place security gateways at the network boundary, perform similar access control on individual information processing devices (servers).	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Communications security" (27K1:2013 A.13; 27K1:2022 A.8.20, A.8.21, A.8.22, A.5.14, A.6.6). • "Securing application services on public networks" (27K1:2013 A.14.1.2; 27K1:2022 A.8.26). • "Logging" (27K1:2013 A.12.4; 27K1:2022 A.8.15). • "Monitoring Activities" (27K1:2022 A.8.16). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-2	Configure security gateways to prevent traffic with unauthorized IP addresses from passing through (e.g., by setting the IP addresses of connecting devices as private addresses and controlling traffic attempting to pass through firewalls, VPN devices, etc., based on IP address).	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-3	In medical information systems limit connections to the services listed below when connecting to services on open networks such as the internet. Use other necessary services only after obtaining agreement from medical institutions: • Remote monitoring and maintenance of medical information systems, etc., from outside • Downloading the latest pattern files for security software • Downloading security patch files for operating systems and applications • Accessing time authentication authorities for electronic signatures, and accessing certification authorities for revocation lists during electronic signature verification • Monitoring unauthorized access to security devices such as firewalls, IDS/IPS • Accessing time distribution servers for time synchronization • Internet services necessary for using these services (e.g., accessing domain name servers) • Other services necessary for the operation of medical information systems (external authentication servers, external medical information databases, etc.). •	
	❷ Prevention of Impersonation.	❷-1	Pre-agree on the methods for exchanging information as follows: • Procedures for exchanging information recorded on electronic media • Procedures for exchanging information via network in document file format • Procedures for exchanging information via network through application input • Methods and verification procedures for affixing electronic signatures and timestamps to information	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Communications security" (27K1:2013 A.13; 27K1:2022 A.8.20, A.8.21, A.8.22, A.5.14, A.6.6). • "Securing application services on public networks" (27K1:2013 A.14.1.2; 27K1:2022 A.8.26). Acronis' certifications to the ISO/IEC 27017 and ISO/IEC 27018 Standards assure its commitment to secure its cloud services and a secure handling of PII into the cloud. Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/company/privacy/ Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❷-2	Ensure the following in information exchange procedures, regardless of the mode of transportation: Identify and record the sender and recipient. Implement non-repudiation measures such as keeping shipping documents, attaching digital signatures to document files, and ensuring authentication at application logon, so that the sender's actions cannot be denied later. Agree on the confidentiality level of the information being exchanged (ensuring that the confidentiality level does not decrease on the recipient's side). Ensure that the exchanged information does not contain any malicious code.	
		❷-3	When transferring information electronically, implement the following measures: • The sender and receiver shall authenticate each other electronically to verify the legitimacy of the counterpart. The authentication method may vary depending on the connection type and application used for transfer, but it is desirable to authenticate both the devices being used and the users themselves. • The transmission path is protected from interception risks through appropriate methods. • Take measures to verify that the received information has not been damaged or altered en route. • In case of transmission failure, attempt retransmission up to a pre-defined number of times. If the limit is reached, halt all communication between the sender and receiver and proceed with identifying the issue.	
		❷-4	In the network from medical institutions to the contracted service provider, verify the path at necessary units such as the entrance and exit points of the sending and receiving sites of medical institutions, the equipment used, functional units on the equipment used, and users.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Communications security" (27K1:2013 A.13; 27K1:2022 A.8.20, A.8.21, A.8.22, A.5.14, A.6.6). • "Securing application services on public networks" (27K1:2013 A.14.1.2; 27K1:2022 A.8.26). Acronis' security teams are focused to keep a robust perimeter securing Acronis' network infrastructure. Internal, continuous testing of the network perimeter is conducted rigorously using various types of penetration tests. Additionally, Acronis coordinates external third-party penetration testing, leveraging qualified and certified penetration testers.
		❷-5	In ❷-4, conduct mutual authentication between the server connected by medical institutions to external networks and the server of the contracted service provider.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❷-6	For ❷-4, if the contracted service provider has subcontracted maintenance work, implement separate measures to prevent impersonation in the connection between the contracted service provider and the subcontractor.	
		❷-7	Agree with medical institutions on verifying that the communication mode authentication methods adopted by medical institutions in Section ❹ of the 'Network-related Security Management Measures' in the Guidelines for the Security Management of Medical Information Systems are reasonable.	
	❸ Restrictions on Unauthorized Device Connections to Network Ports.	❸-1	Restrict physical connections to unused network ports on network devices, servers, and terminals.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). • "Equipment siting and protection" (27K1:2022 A.11.2.1; 27K1:2022 A.7.8). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❸-2	Create and maintain a list registering information processing devices used within medical information systems to identify unauthorized devices.	
		❸-3	To avoid the adverse effects of unauthorized information processing devices connecting to the network, ensure consistency with registered network addresses and guard against malicious intentions.	
	❹ Measures When Using Wireless LAN.	❹-1	When medical institutions use wireless LAN in services handling medical information, agree with medical institutions on the necessary security measures and the division of roles among medical information system operators, etc.	Not applicable. This is the customer's responsibility to respond to.
		❹-2	When taking mobile devices storing information related to medical information systems out for business purposes, do not connect to public wireless LANs.	Not applicable. This is the customer's responsibility to respond to.
3.9. Detection and Blocking of Unauthorized Communi-cations.	❶ Detection and Blocking of Unauthorized Communications on the Network.	❶-1	Install Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), etc., at the network boundary connecting with medical institutions to detect unauthorized events on the network or block unauthorized traffic. When using hosting services or in cases where it is not possible to install devices at the network boundary, perform similar controls on individual information processing devices.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Logging" (27K1:2013 A.12.4; 27K1:2022 A.8.15). • "Monitoring Activities" (27K1:2022 A.8.16). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). • "Access to networks and network services" (27K1:2013 A.9.1.2; 27K1:2022 A.5.15). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-2	Ensure that intrusion detection systems and similar technologies are always capable of responding to the latest attacks and unauthorized access by updating signatures, detection rules, and applying security patches to the software.	
		❶-3	Configure intrusion detection systems and similar technologies to immediately notify administrators via output to monitoring terminals or through emails when detecting attacks or unauthorized access activities of high urgency.	
		❶-4	Include necessary items in the records of intrusion detection that are required for the post-processing of unauthorized access and similar incidents.	
		❶-5	It is recommended to monitor at the network boundary to ensure that no unauthorized or suspicious traffic is flowing from the internal network of medical information systems to the external network.	
		❶-6	It is recommended to implement settings that hide the presence of intrusion detection systems from external observation (stealth mode) and to properly control access to these systems to prevent them from becoming targets of attacks and unauthorized access.	
		❶-7	When providing services that include the use of IoT devices, record the access status to medical information systems, etc., by IoT devices and regularly monitor to ensure there is no unauthorized access.	Not applicable. This is the customer's responsibility to respond to.
3.10. Management of Devices and Information Taken Outside.	❶ Authentication of Devices Taken Outside.	❶-1	Set a startup password for devices.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: ▪ “Access Control” (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). ▪ “Security of equipment and assets off-premises” (27K1:2013 A.11.2.6; 27K1:2022 A.7.9). ▪ “Equipment siting and protection” (27K1:2022 A.11.2.1; 27K1:2022 A.7.8). ▪ “Equipment maintenance” (27K1:2013 A.11.2.4; 27K1:2022 A.13). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report.
		❶-2	Implement measures to prevent unauthorized device startup by third parties, such as setting difficult-to-guess startup passwords and changing them periodically according to the characteristics of the device.	
		❶-3	For logging into and accessing information devices that store information related to medical information systems use a combination of multiple authentication factors.	
	❷ Measures for Information Being Transported.	❷-1	When taking devices or media storing information outside, the procedures should include encrypting the device or media itself, applying encryption measures to the stored information, and setting passwords, among other measures.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: ▪ “Access Control” (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). ▪ “Security of equipment and assets off-premises” (27K1:2013 A.11.2.6; 27K1:2022 A.7.9).

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.11. Measures Against Information Leakage through Virtual Desktops, MDM (Mobile Device Management), and MAM (Mobile Application Management).	❶ Management of Personally Owned Devices.	❶-1	Agree with medical institutions on countermeasures for the use of medical information systems via devices personally owned by users. Specifically, consider the following measures: • From the perspective of preventing information leakage from devices owned by users, for example, use virtual desktops to separate business and personal use areas at the OS level, allowing medical institutions to manage the business use area. Additionally, applying Mobile Device Management (MDM) or Mobile Application Management (MAM) can ensure security measures equivalent to those on devices owned and managed by medical institutions, etc.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • "Security of equipment and assets off-premises" (27K1:2013 A.11.2.6; 27K1:2022 A.7.9). • "Remote working" (ISO27K1:2013 A.6.2.2; ISO27K1:2022 A.6.7). Employees at Acronis are furnished with Acronis machines and mobile devices for business purposes. Moreover, Acronis permits the use of Acronis' fully managed applications on user-owned devices for business activities.
		❶-2	As a principle, prohibit the use of personally owned devices by employees and others for purposes related to the provision of services (including development, maintenance, and operation).	
	❷ Implementation of Technologies that Leave No Information on the Terminal.	❷-1	Agree with medical institutions on the division of responsibilities of contracted service providers for implementing technologies like virtual desktops in the PC work environment used by users of medical institutions when accessing services from outside the medical institutions.	• Not applicable. This is the customer's responsibility to respond to.
3.12. Restriction of Unregistered Electronic Media Connections.	❶ Restriction on Connecting Unregistered Electronic Media to Servers.	❶-1	In medical information systems limit the types of electronic media that can connect to servers by removing unnecessary device drivers. Additionally, to prevent the connection of unauthorized types of devices, it is desirable to configure settings so that only administrators can install or uninstall device drivers.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • "Configuration Management" (27K1:2022 A.8.9). • "Virtual Machine Hardening" (27K17:2015 CDL.9.5.2). Acronis' Cyber Cloud Infrastructure is a code-base infrastructure deployed from a trusted and verified baseline. Additionally, tools are employed to identify variances from predefined operating system (OS) configurations on production machines and rectify them automatically.
		❶-2	It is recommended to regularly verify that unnecessary device drivers have not been added.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.13. Use of Encryption and Electronic Signatures.	❶ Use of Verified Safe Encryption and Electronic Signatures.	❶-1	In the network, take necessary measures (such as establishing standards and procedures for information exchange, encrypting communications, etc.) to protect against eavesdropping, tampering, misrouting, destruction, and other threats to information.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis implements encryption and authentication for all data in transit across one or more network layers whenever data is transmitted beyond physical boundaries not under Acronis' control or on Acronis' behalf. For further details on Acronis' security posture, please visit https://www.acronis.com/resource-center/resource/acronis-cloud-data-centers-a-primer-on-security-privacy-and-compliance/.
		❶-2	Implement necessary measures (such as the introduction of server certificates) to prevent impersonation of access destinations (session hijacking, phishing, etc.).	
		❶-3	Agree with medical institutions on ensuring the security of communication paths, including support for IPsec + IKE, closed network environments, and their specific requirements.	
		❶-4	It is recommended to consider the risk of direct interception for the cables used in information transmission.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). • "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report.
		❶-5	Use encryption algorithms that have sufficient security. The Electronic Government Recommended Cryptography List, among others, can be used as a selection criterion.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		❶-6	Implement security measures, such as encryption, for the information itself between the sender and the recipient.	
		❶-7	When using SSL/TLS in service provision, take measures that are compatible with TLS 1.2.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). Acronis endorses the adoption of open encryption methodologies and mandates TLS for all authentication traffic. Customer data undergoes encryption while traversing Acronis' internal networks, both during transit and at rest.
		❶-8	In addition to ❶-7, if medical institutions require email encryption (such as S/MIME) or file encryption, agree with them on the necessary measures and conditions for such support.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		1-9	When establishing a VPN connection, adhere to the following: Perform mutual authentication between VPN devices at the time of connection. Use appropriate cryptographic technologies to minimize the risk of interception, replay attacks, etc. Ensure that traffic on the internet does not mix into the VPN channel by not setting a direct path between the private network interface and the internet interface. If entrusted with information processing tasks from multiple medical institutions, etc., implement measures such as constructing separate VPN channels for each medical institution to avoid the risk of information confusion among them.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). • "Securing application services on public networks" (27K1:2013 A.14.1.2; 27K1:2022 A.8.26). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		1-10	When connecting via HTTPS over an open network, configure TLS settings for both server and client to conform to the most secure 'High Security Type' as defined in the 'SSL/TLS Encryption Settings Guidelines,' ensuring the highest level of security.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). Acronis endorses the adoption of open encryption methodologies and mandates TLS for all authentication traffic. Customer data undergoes encryption while traversing Acronis' internal networks, both during transit and at rest.
		1-11	As a principle, do not use SSL-VPN.	
		1-12	When providing services and connecting via software-based IPsec or TLS 1.2, implement appropriate measures to protect against attacks such as session hijacking (access to closed sessions through routes that are not the legitimate path).	
		1-13	When users at medical institutions connect via software-based IPsec or TLS 1.2, provide them with information on appropriate measures against attacks such as session hijacking (access to closed sessions through routes that are not the legitimate path). Agree with the medical institutions on the scope and conditions of the information provided.	
	2 Management of Cryptographic Keys and Electronic Signatures to Mitigate the Risks Associated with Compromised Encryption Algorithms and Key Leakage.	2-1	Develop contingency plans in preparation for potential cryptographic key leakage.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). • "Data leakage prevention" (27K1:2022 8.12). • "Information security incident management planning and preparation" (27K1:2013 A.16.1.1; 27K1:2022 A.5.24). • "Assessments and decisions on information security events" (27K1:2013 A.16.1.4; 27K1:2022 A.5.25). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		2-2	When using electronic certificates for electronic signatures, network connections, etc., ensure that the electronic certificates are issued by a trustworthy organization.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). • "Networks Security" (27K1:2013 A.13.1; 27K1:2022 A.8.20, A.8.21, A.8.22). Certificates are used by Acronis to assure authentication integrity.
		2-3	Take into consideration the ability to switch cryptographic algorithms in preparation for the compromise of cryptographic algorithms and keys.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). • "Data leakage prevention" (27K1:2022 8.12). • "Information security incident management planning and preparation" (27K1:2013 A.16.1.1; 27K1:2022 A.5.24). • "Assessments and decisions on information security events" (27K1:2013 A.16.1.4; 27K1:2022 A.5.25). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
		2-4	Obtain the root certificate authority's public key certificate through a secure channel for verifying data received from medical institutions and compare it with a fingerprint obtained through a different route to verify its authenticity.	Not applicable. This is the customer's responsibility to respond to.
		2-5	When cryptographic modules use external source code or libraries, it is recommended to use them only after verifying their integrity through methods such as electronic signatures provided by the manufacturer to ensure authenticity.	Not applicable. This is the customer's responsibility to respond to.
		2-6	It is recommended to generate cryptographic keys in a secure environment, using tamper-resistant devices such as IC cards or USB token devices.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24).
		2-7	When making provisions for key escrow in case of cryptographic key loss, it is recommended to implement access controls to ensure that only legitimate administrators and processes can access the cryptographic key repository.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24). Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • "Use of cryptography" (27K1:2013 A.10.1; 27K1:2022 A.8.24).
		2-8	In environments where electronic signatures applied to documents by medical practitioners are verified in accordance with the Electronic Signature Law, it is desirable to ensure that signature verification can continue without being affected by the weakening of cryptographic algorithms.	Not applicable. This is the customer's responsibility to respond to.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.14. Access Management for Remote Maintenance.	❶ Access management to prevent unnecessary logins during remote maintenance.	❶-1	When performing remote maintenance, take appropriate security management measures as necessary, such as setting up appropriate access points, limiting protocols, and managing access permissions.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Access Control" (27K1:2013 A.9; 27K1:2022 A.5.15, A.5.16, A.5.17, A.5.18, A.8.2). • "Change management" (27K1:2013 A.12.1.2; 27K1:2022 A.8.32). • "System acquisition, development and maintenance" (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). Information security oversight and management controls are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure, manage and protect their environment.
3.15. Management When Using Electronic Signatures.	❶ Use of Electronic Certificates Issued by Trustworthy Third-Party Institutions.	❶-1	When using electronic signatures in medical information systems use electronic certificates issued by trustworthy third-party institutions, such as signature electronic certificates issued by the PKI (Public Key Infrastructure) Certification Authority in the health, medical, and welfare fields.	Not applicable. This is the customer's responsibility to respond to.
	❷ Attaching Timestamps When Applying Electronic Signatures.	❷-1	When applying electronic signatures to information, attach timestamps. In this case, agree with medical institutions on the contents of the timestamps and the method of verification.	Not applicable. This is the customer's responsibility to respond to.
		❷-2	When handling information to which timestamps have been attached, agree with medical institutions on the methods for verifying the validity of these timestamps within the statutory retention period, as well as on the response methods.	Not applicable. This is the customer's responsibility to respond to.
		❷-3	When handling information to which timestamps have been attached, agree with medical institutions on measures to be taken for the long-term preservation of such information.	Not applicable. This is the customer's responsibility to respond to.
	❸ Use of Valid Electronic Certificates at the Time of Attaching Timestamps Use of Valid Electronic Certificates at the Time of Attaching Timestamps.	❸-1	When handling information to which timestamps have been attached, agree with medical institutions on the method of attaching timestamps to ensure the validity of electronic signatures made before the expiration of the electronic certificate.	Not applicable. This is the customer's responsibility to respond to.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.16. Implementation of Tamper Prevention and Detection Measures.	❶ Implementation of Tamper Prevention and Detection Measures for Software.	❶-1	To verify that software has not been tampered with, regularly conduct software integrity checks (tamper detection).	Acronis is certified to the ISO 9001 and ISO/IEC 27001 Standards, which regulate: • "Change management" (27K1:2013 A.12.1.2; 27K1:2022 A.8.32) • "System acquisition, development and maintenance" (27K1:2013 A.14; 27K1:2022 A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.32). • "Design and development of products and services" (9001:2015 8.3). Acronis established a Security Development Life Cycle (SDLC) to assure multiple software security checks from the design to the deployment. A bug bounty program is run to involve independent security researchers. Information security oversight and management controls, including change management and software developing, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Customers using Acronis Cyber Protect Cloud retain all rights and responsibilities to configure and manage their environment, including change management and system development procedures.
			To avoid the risk of unauthorized software modification, implement tamper prevention and detection measures for the software when deploying it to operational facilities.	
3.17. Management of Information for Each Patient.	❶ Implementation of Functions for Managing Information on a Per-Patient Basis.	❶-1	Include in medical information systems the functionality to manage the medical information entrusted to each patient or similar individual.	Not applicable. This is the customer's responsibility to respond to.
3.18. Ensuring Response Times According to the Purpose of Use.	❶ Ensuring Response Times According to the Purpose of Use of Medical Information Systems.	❶-1	Agree with medical institutions on the response times (such as general display speed, search result display time, etc.) when using medical information systems.	Not applicable. This is the customer's responsibility to respond to.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.19. Fault Tolerance Measures through Redundancy.	❶ Implementing Redundancy Measures to Ensure Continuity in the Event of Medical Information System Downtime.	❶-1	To ensure business continuity even in the event of a failure in information processing equipment, implement measures such as preparing alternative devices, redundancy, and establishing backup facilities.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Information Security during disruption” (27K1:2013 A.17.1; 27K1:2022 A.5.39) • “ICT readiness for business continuity” (27K1:2022 A.5.30) • “Information Backup” (27K1:2013 A.12.3.1; 27K1:2022 A.8.13) • “Redundancy of information processing facilities” (27K1:2013 A.17.2.1; 27K1:2022 A.8.14) Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This “redundancy in all aspects” strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers’ content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data, and if available, enable additional georedundancy services according to their own business continuity and disaster recovery strategies. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/.
		❶-2	For medical information systems and networks, take the necessary redundancy measures to ensure the continuity of services without affecting normal medical practices.	
		❶-3	Considering ❶-2, agree with medical institutions on the level of service continuity guaranteed in the event of a failure or other incidents.	
		❶-4	Agree with medical institutions on alternative measures on their part to ensure that medical practices can continue even in the event of a failure or similar situations.	
	❷ Disk Failure Measures.	❷-1	When saving information such as medical records on recording devices like hard disks, implement disk failure measures equivalent to or beyond RAID-1 or RAID-6.	Acronis stores customer data by employing its own software-defined storage solution, Acronis Cyber Infrastructure with Acronis CloudRAID technology. Acronis Cyber Cloud Infrastructure delivers fast, universal, protected, efficient and proven storage that unites block, file and object workloads.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.20. Measures in the Event of System Failure.	❶ Implementation of Functions in the Event of a Medical Information System Failure.	❶-1	Agree with medical institutions on providing information about possible measures that can be taken by the medical institutions to ensure readability of medical information in the event of a failure when storing medical information at medical institutions.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39) • "ICT readiness for business continuity" (27K1:2022 A.5.30) • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13) • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14) Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy — where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers' content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data, and if available, enable additional georedundancy services according to their own business continuity and disaster recovery strategies. Acronis highly recommends customers adopt. a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/.
		❶-2	Evaluate the magnitude of the impact posed by hardware and software, and for components with too great an impact, implement redundancy for those system components or prepare for situations where system failure renders information inaccessible by ensuring it can be viewed through generic browsers or similar means.	
		❶-3	Agree with medical institutions on the availability and specifics of functions for outputting external files and the like, necessary to ensure readability in the event of a failure when storing medical information at medical institutions.	
		❶-4	Agree with medical institutions on the functions for utilizing backup data stored remotely to ensure readability in the event of a failure, the provision of information necessary for its use, and other conditions, when storing medical information at medical institutions.	
		❶-5	Include in the service functions that support ensuring the readability of medical records and similar documents in emergency situations at medical institutions, such as printing capabilities and file downloading features. Agree with medical institutions on providing information necessary for these functions, including security requirements.	
		❶-6	Clarify the division of responsibilities in the event of a failure or similar incident and agree with medical institutions on the scope of services that guarantee operation.	Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/company/privacy/ https://www.acronis.com/legal/
3.21. Management of Backup and Restoration.	❶ Management of Information for Backup and Restoration.	❶-1	To minimize the risk of information loss due to damage to electronic media, store them in the storage conditions specified by the manufacturer of the electronic media.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Physical and environmental security" (27K1:2013 A.11; 27K1:2022 A.7.1, A.7.2, A.7.3, A.7.4, A.7.5, A.7.6). Information security oversight and management controls, including physical security management practices are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-2	Take measures to provide, at any time, information on the remaining capacity of storage resources available to each medical institution.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • “Capacity Management” (27K1:2013 A.12.1.3; 27K1:2022 A.8.6; 27K17 12.1.3).
		❶-3	When medical institutions use medical information systems, agree with them on information related to available resources (storage capacity, availability period, risks, backup frequency, backup methods, etc.).	
		❶-4	Include the locations where the medical information system stores information (internally, on portable media), the storage capacity available for each location, the storage period, risks, etc.	Acronis is certified to the ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018 Standards, which regulate: • “Capacity Management” (27K1:2013 A.12.1.3; 27K1:2022 A.8.6; 27K17:2015 12.1.3). • “Contact with authorities” (27K1:2013 A.6.1.3; 27K1:2022 A.5.5; 27K17:2015 6.1.3). • “Geographical location of PII” (27K18:2019 A.12.1). • “Segregation in virtual environments” (27K17:2015 CLD.9.5.1). Information security oversight and management controls, including physical security management practices are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report.
		❶-5	In item ❶-4, even when using medical information systems provided by other businesses, collect similar information and respond accordingly. When using medical information systems through virtualization technology, the contracted service provider confirms information about resources available under contracts with other businesses.	
		❶-6	Conduct education for employees on the management methods defined in the operational management policies pursuant to item ❶-4.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Documented Operating Procedures” (27K1:2013 A.12.1.1; 27K1:2022 A.5.37). • “Information security awareness, education and training” (27K1:2013 A.7.2.2; 27K1:2022 A.6.3) Acronis upholds comprehensive internal documentation and adheres to an Information Security Management System (ISMS), in compliance with ISO 27001 standards. All documents are stored on systems that are replicated and backed up. All Acronis contractors receive security training as an integral part of their induction process and continue to receive training throughout their tenure at Acronis. As part of their orientation, new contractors commit to our Code of Conduct, emphasizing our dedication to protecting customer information securely. Based on their specific roles, they may undergo additional training on particular security facets. Information security oversight and management controls, including management of security awareness and training are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report.
		❶-7	For contracted service providers involved in medical information systems, demand compliance with the management methods defined in the operational management policies pursuant to item ❶-4.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-8	Take measures to quickly recover information in case of corruption and include the content and procedures for recovery in the operational management policies and procedures.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39). • "ICT readiness for business continuity" (27K1:2022 A.5.30). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers' content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data, and if available, enable additional georedundancy services according to their own business continuity and disaster recovery strategies. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/.
		❶-9	Include in the operational management policies and procedures measures for scenarios where information cannot be recovered despite the measures outlined in ❶-8.	
		❶-10	Agree with medical institutions on the scope of responsibility and conditions for exemption in cases of damaged information as outlined in ❶-9.	Please refer to the following documents which outline contractual obligations and agreements: https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/company/privacy/ https://www.acronis.com/legal/ https://www.acronis.com/support/eula/.

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-11	Based on the results of a risk analysis, backups of the medical information system and related systems are obtained. Define the targets for backup acquisition, the frequency of backups, methods and media for storage, and management methods. Include these details in operational management policies and procedures.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39). • "ICT readiness for business continuity" (27K1:2022 A.5.30). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers' content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data, and if available, enable additional georedundancy services according to their own business continuity and disaster recovery strategies. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/.
		❶-12	Conduct regular inspections and other necessary measures according to the management method of the recording media for obtained backups, to ensure that there is no tampering or destruction of the recorded content.	
	❷ Management of Media Used for Backups.	❷-1	For backups stored on recording media, manage the content of the backup, the start date of use, and the end date of use, considering the characteristics of the media (type of tape/disk, capacity, etc.).	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • "Information Security during disruption" (27K1:2013 A.17.1; 27K1:2022 A.5.39). • "ICT readiness for business continuity" (27K1:2022 A.5.30). • "Information Backup" (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • "Redundancy of information processing facilities" (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis' SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This "redundancy in all aspects" strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis does not duplicate customers' content data; each customer using Acronis Cyber Protect Cloud has the sole responsibility to choose where to store their own data, and if available enable the georedundancy additional service, according to their own business continuity and disaster recovery strategies. Acronis highly recommends customers adopt a 3-2-1 backup strategy. For more information on 3-2-1 backup strategy, please check https://www.acronis.com/blog/posts/backup-rule/.
		❷-2	When the end date of use for the backup recording media approaches, copy the content to another medium or similar before the end date.	
		❷-3	When the effective usage limit period of electronic media, as set by the manufacturer, approaches, copy the data to another medium or similar to ensure it does not exceed the effective usage limit period.	
		❷-4	Include the procedures from ❷-1 to ❷-3 in the operation management policies and provide necessary training to employees and subcontractors.	
		❷-5	Agree with medical institutions on the provision of information related to backups.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
3.22. Ensuring compatibility for system change and improvement.	❶ Ensuring Compatibility of Data Formats and Protocols.	❶-1	For data items such as medical records, the standards for the field of health and medical information in the MHLW (hereinafter referred to as "MHLW standards") shall be adopted.	Not applicable. This is the customer's responsibility to respond to.
		❶-2	For data items not defined by the MHLW standards, they should be in an easily convertible data format, and an agreement should be reached with medical institutions and related entities.	Not applicable. This is the customer's responsibility to respond to.
		❶-3	When modifying master tables related to medical information, the medical information system should include functions and verification methods that ensure changes do not occur in the records of medical records and other information, regarding the method of managing records and the actions to be taken.	Not applicable. This is the customer's responsibility to respond to.
		❶-4	If it is difficult to equip the medical information system with the functions and methods mentioned in ❶-3, agree on the procedures for updating or migrating the medical information system with medical institutions.	Not applicable. This is the customer's responsibility to respond to.
		❶-5	When the data format and protocol for storing and exchanging medical information are changed, as long as there are medical institutions using the previous data format and protocol, maintain compatibility with the previous data format and protocol.	Acronis as a company differentiates between two types of data: Data necessary for providing the services (e.g., product usage) and Acronis' service management. This is the data that Acronis collects and processes as a data controller for providing our services. Such data may include account names, email and other contact details, billing details, and some information automatically collected via the service, which may be personal. For more details, please check Acronis Privacy Statement: https://www.acronis.com/company/privacy/ Customers' content data. This is the data that Acronis may process as a data processor (subprocessor) when you use our services. The information is provided by customers while utilizing the specific products — e.g., backup archives, files, virtual machines, etc. In terms of this type of data, Acronis does not control the categories and the content of the information which customers are storing with us. Customers are solely responsible for evaluating and maintaining their own legal and compliance obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with its customers, who have such obligation under applicable data protection regimes.
		❶-6	When upgrading or changing the data format or transfer protocol, confirm the impact on service usage.	
		❶-7	If it is recognized that the results of ❶-6 affect the use of services, notify the upgrade or change with sufficient time for medical institutions to make adjustments, and provide specific information on the measures needed for response.	
		❶-8	❶-7 should be carried out considering data linkage with other medical information systems. Agree with medical institutions on providing information related to ensuring compatibility for them.	

Category	Sub-Category	No.	Content of the requirement	Acronis compliance
		❶-9	If medical institutions decide to discontinue the use of services as a result of changes in data formats and transfer protocols, measures will be taken to ensure readability.	Acronis is certified to the ISO/IEC 27001 and ISO/IEC 27017 Standards, which regulate: • “Return of the assets” (27K1:2013 A.8.1.4; 27K1:2022 A.5.11). • “Removal of cloud service customer assets” (27K17:2015 CLD.8.1.5). Acronis’ Platform Terms of Service delineates contractual responsibilities and agreements. Please refer to section 9.7 of https://www.acronis.com/support/platform-terms-conditions/.
		❶-10	Devices and software related to medical information systems shall be selected with future compatibility in mind, and risks associated with changes to standard specifications after the provision of services shall also be considered.	Not applicable. This is the customer’s responsibility to respond to.
		❶-11	When a service is provided using medical information systems provided by another service providers, measures are taken to prevent a problem from occurring in the contractors’ service provision even when another providers stop the services. In case some or all of the services provided by another providers are stopped or changed (minor version upgrades are not included) due to the stoppage or change of the service of another providers, take countermeasures to prevent equipment from deteriorating.	Acronis is certified to the ISO/IEC 27001 Standard, which regulates: • “Information Security during disruption” (27K1:2013 A.17.1; 27K1:2022 A.5.39). • “ICT readiness for business continuity” (27K1:2022 A.5.30). • “Information Backup” (27K1:2013 A.12.3.1; 27K1:2022 A.8.13). • “Redundancy of information processing facilities” (27K1:2013 A.17.2.1; 27K1:2022 A.8.14). Information security oversight and management controls, including business continuity practices, are reviewed and verified by a third-party auditor for Acronis’ SOC 2, Type II report. Acronis designs the elements of its platform with high redundancy, where at least an N+1 paradigm is adopted. This approach is evident in the architecture of its servers, data storage practices, network and internet connections and the software services provided. This “redundancy in all aspects” strategy ensures error management is built into the system, offering a solution that does not rely on a singular server, data center or network connection. Acronis has established partnerships that run numerous global, colocated data center facilities. These facilities meet rigorous standards and compliance needs regarding setup, power and cooling. This approach maintains optimal conditions and uptime to safeguard mission-critical data. Additionally, Acronis has strict requirements for data center locations to reduce or eliminate the probability of the most typical disruptive events. During the term of each contract, Acronis regularly monitors and reviews the third party’s security controls, service delivery and compliance with contractual requirements.
		❶-12	When updating devices or software related to medical information systems, or when changing the services of other businesses used, consider items ❶-10 and ❶-11 in doing so.	Not applicable. This is the customer’s responsibility to respond to.

Acronis

For more information
visit www.acronis.com