Acronis

WHITE PAPER

Demystifying 2G3M

Health data compliance in Japan

Table of contents

Disclaimer

The purpose of this white paper is to provide opinion and current understanding of the importance, implications and implementation of cybersecurity policies, procedures and best practices associated with the second edition of the Two Guidelines from Three Ministries (2G3M). In the creation of this white paper, we have relied on the official published version of the complete document in Japanese as found on the official websites. We have made every effort to be as accurate and thorough as possible, but as with all such matters, the information is subject to interpretations, revisions and clarifications over time. The authors advise all readers to review the source material and consult with relevant legal and regulatory experts to form their own conclusions.

Scenario

Japan has been actively advancing digital transformation initiatives through government-led strategies such as the Society 5.0 vision and the Digital Agency's reforms. These initiatives emphasize the integration of AI-driven technologies, cloud computing and data interoperability to modernize various sectors, including health care. The adoption of these technologies has been strongly promoted, enabling IT vendors to play a crucial role in Japan's transition toward a secure, interconnected, and technology-driven society. In particular, the health care sector benefits from these advancements through enhanced electronic health record (EHR) management, secure patient data exchange, and real-time diagnostics.

Japan's cybersecurity strategy has evolved significantly over the years, with a strong emphasis on protecting critical sectors and personal data. The 2G3M framework, which consists of Two Guidelines from Three Ministries, is specifically designed as a comprehensive cybersecurity framework for handling health data. It provides structured guidance to mitigate emerging threats, enhance risk management and align with Japan's broader cybersecurity objectives.

The 2G3M framework comprises two key cybersecurity guidelines issued jointly by three government ministries:

Guideline for Safety Management of Medical Information Systems, Version 6

Issued by the Ministry of Health, Labor and Welfare (MHLW), this guideline provides directives for ensuring the security and integrity of health care information systems.

LEARN MORE

1

Safety Management Guideline for Information Systems and Service Providers Handling Medical Information, Version 1.1

Issued by the Ministry of Economy, Trade, and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC), this guideline focuses on ensuring safe practices among IT service providers managing medical information.

LEARN MORE

2

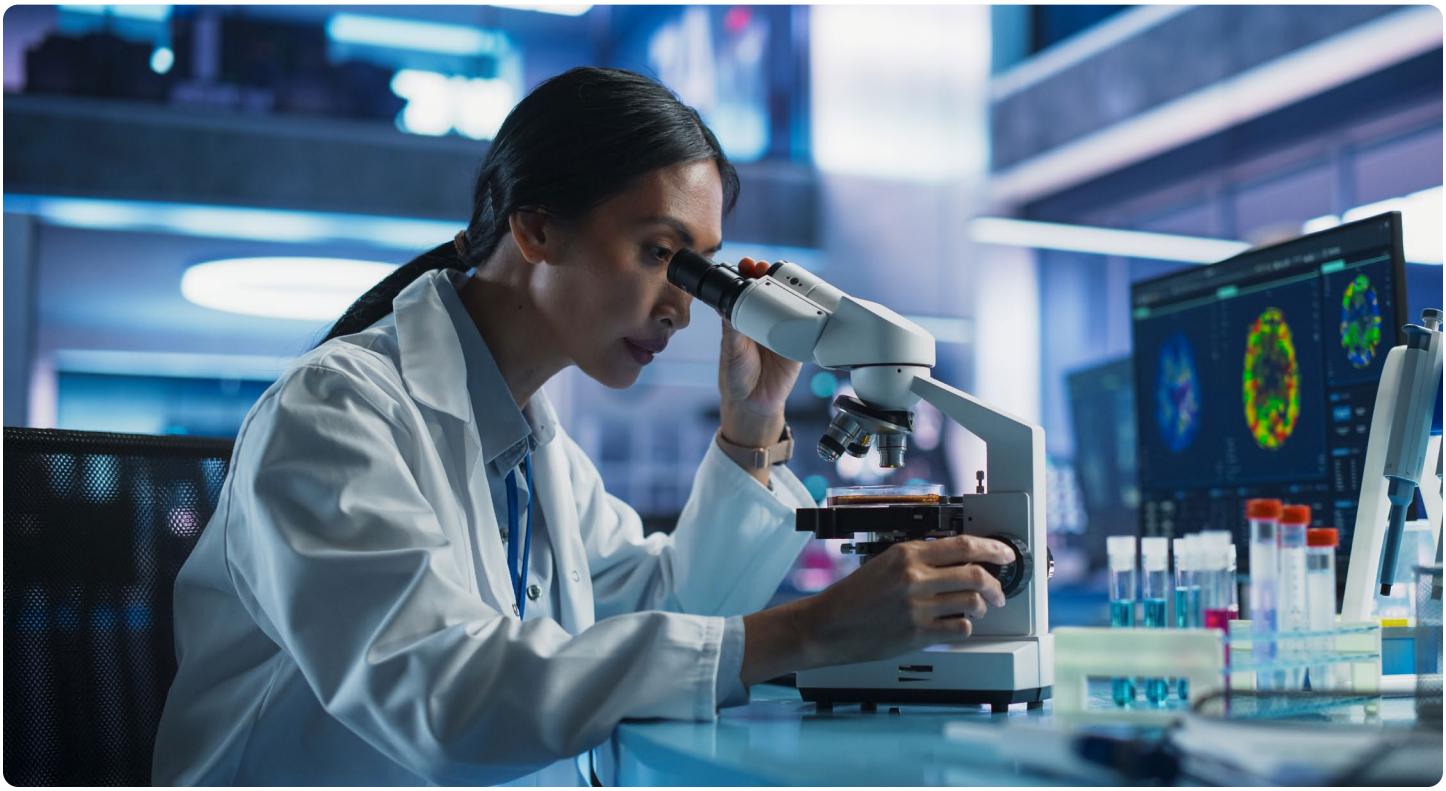
Due to its focus on health data protection, the 2G3M framework is closely related to the Act on the Protection of Personal Information (APPI). While APPI establishes general data protection obligations across industries, 2G3M provides specific cybersecurity and risk management measures for entities handling medical information.

Who must comply with 2G3M

Under the APPI, three primary roles are defined in data handling: Personal Information Handling Business Operator, Entrusted Person and Subcontractor. These classifications help determine which entities should adopt 2G3M by aligning cybersecurity requirements with their responsibilities in handling medical information.

- **Personal Information Handling Business Operators** (PIHBOs) are the primary entities responsible for collecting and managing personal data, such as hospitals and health care providers (clinics, pharmacies, maternity homes, home-visiting nursing stations, care providers, etc.). Under 2G3M, they are required to implement comprehensive cybersecurity governance, risk management policies and technical safeguards to protect patient information.
- **Entrusted Persons** are organizations or individuals that handle personal data on behalf of PIHBOs. For example, cloud-based electronic health record (EHR) platforms that store and manage patient records must comply with 2G3M by enforcing strict access controls, encryption policies and cybersecurity incident response mechanisms.
- **Subcontractors** are third-party vendors further down the supply chain, such as software developers, infrastructure providers and data processors. Even though they may not directly manage patient data, they must adhere to 2G3M security requirements to ensure the integrity and confidentiality of medical information throughout the supply chain.

By integrating APPI's role-based classifications, 2G3M establishes a structured compliance model that ensures every entity involved in health care data processing maintains high cybersecurity standards. The ultimate responsibility for compliance under 2G3M lies with PIHBOs such as hospitals and health care institutions, as they directly manage and oversee the collection, storage, and protection of sensitive medical data. However, this responsibility is shared with Entrusted Persons, such as IT service providers, who must implement the required cybersecurity controls when processing data on behalf of PIHBOs. Likewise, Subcontractors must ensure compliance with relevant security measures to maintain the integrity of medical information throughout the supply chain.



How to adopt 2G3M

The adoption of 2G3M is a fundamental and critical step for entities managing medical information systems in Japan. While the second guideline is dedicated to external storage services providers for medical information such as electronic medical records (EMRs), cloud-based EMR services, online medical consultation systems, etc., the first guideline is broadly applied to all information systems handling medical data. So, the framework outlines best practices, compliance requirements and governance structures to enhance cybersecurity resilience within the health care sector.

Step 1

The first step is understanding who you are and what your role is in the health data handling process. This is crucial, as without a clear self-understanding, it is not possible to claim compliance or assume that other parties are following certain requirements. In order to gain such understanding, you could try answering the following questions:

- Are you a health care provider, a medical institution, a system vendor or a third-party service provider handling medical data?
- What type of medical data do you process, and in what capacity (e.g., patient records, diagnostic information, insurance data or medical device telemetry)?
- Do you store, transmit or analyze medical information, and what are your security responsibilities in each phase?
- Which regulations are you already applying to your operations (e.g., APPI, Medical Practitioners' Act, or relevant METI and MHLW guidelines)?
- Are you directly responsible for the information security controls, or do you rely on third-party services for compliance?

Step 2

Having clarified your role on the data you handle, and how you are doing it, you can proceed with the second step, which is to verify your compliance against 2G3M requirements. The three ministries have published several FAQs and checklists you can use to evaluate your compliance; my personal suggestion is to begin with the "Attachment 2 List of countermeasure items in pre-integration guidelines and correspondence table of medical information safety management guidelines version 6.0." This matrix gives a clear and comprehensive list of the requirements from both guidelines and offers a unique view to choose which of the two guidelines you should follow as primary terms for compliance, according to your status. When analyzing each requirement, the key is to always keep in mind how it applies to your role in health data management.

Step 3

The last step consists of filling the gaps you identified and continuously monitoring that everything is running according to your policies and procedures.

2G3M requirements breakdown

Per Attachment 2, the requirements are divided into three domains:

Human and Organizational

These controls pertain to organizational security and personnel security.

- **Organizational security:** Involves establishing, operating and documenting an organizational structure to oversee security management, including a business continuity program (BCP), risk management and compliance with regulatory frameworks.
- **Personnel security:** Ensures that staff members uphold confidentiality, undergo security awareness training and adhere to access control policies to prevent unauthorized data exposure.

Physical

This involves implementing physical access controls, such as barriers, locks and biometric authentication, alongside environmental security measures to regulate access to data centers, critical IT infrastructure and medical storage.

Technical

This domain covers digital access controls, including authentication, authorization and privilege management, alongside advanced cybersecurity measures such as logging, encryption, data leak prevention (DLP), vulnerability management, intrusion detection / prevention systems (IDS / IPS) and continuous threat monitoring.

Notably, this schema follows the ISO/IEC 27001:2002 Annex A controls organization.

Across all three domains, to achieve 2G3M compliance, It's strongly recommended that you focus on:

1. Risk-based security governance

- Define a security governance framework that aligns with regulatory requirements.
- Assign roles and responsibilities for information security management.
- Establish and maintain a risk management process to evaluate evolving cybersecurity threats.

2. Access control and identity management

- Implement role-based access control (RBAC) and multifactor authentication (MFA).
- Define privilege management policies to limit administrative access.
- Ensure periodic access reviews and audit logs to track system access.

3. Data protection and encryption

- Encrypt sensitive medical data both in transit and at rest.
- Implement data classification policies for handling confidential information.
- Enforce data loss prevention (DLP) measures to prevent unauthorized transfers.

4. Incident response and business continuity

- Develop a security incident response plan (SIRP) to handle security breaches.
- Maintain a disaster recovery (DR) plan to ensure system availability during disruptions.
- Conduct regular cybersecurity drills and penetration testing.

5. Continuous monitoring and threat detection

- Deploy security information and event management (SIEM) solutions for real-time threat detection.
- Implement endpoint detection and response (EDR) solutions to monitor and mitigate threats on workstations and mobile devices.
- Conduct regular vulnerability assessments and penetration testing.
- Maintain automated patch management to address security vulnerabilities.

6. Third-party and vendor risk management

- Establish a third-party risk management (TPRM) framework to assess security risks from external vendors and suppliers.
- Require security assessments, audits and certifications (e.g., ISO 27001, SOC 2, NIST CSF) before onboarding vendors.
- Implement contractual security clauses, including data protection agreements (DPAs) and incident response obligations.
- Continuously monitor vendor security posture through periodic audits, compliance reviews and threat intelligence feeds.
- Enforce access control restrictions for third-party personnel, ensuring least privilege access principles.

All the topics on the list are important, but point six on supply chain security is the topic of the moment. Demonstrating compliance with a recognized standard is crucial for both sides of the supply chain to establish trust.

This raises the ultimate question regarding 2G3M adoption: After a company has implemented all the measures discussed in this white paper, how can it demonstrate compliance with 2G3M?

Currently, there is no official certification issued for the Two Guidelines from Three Ministries. However, these guidelines have been developed with strong alignment to internationally recognized standards — particularly, ISO/IEC 27001, 27017 and 27018.

Therefore, the most practical, effective and market-recognized approach would be to obtain certification from a well-qualified, independent and accredited auditor against the ISO/IEC 27001 family of standards. Organizations can then map 2G3M controls to the corresponding ISO controls, ensuring compliance while leveraging an internationally accepted certification framework.

Benefits of Acronis Cyber Protect in 2G3M environments

Acronis Cyber Protect natively integrates backup with cybersecurity and endpoint management to provide end-to-end cyber resilience, essential for 2G3M environments:

- **Data protection and backup solutions:** Secure patient data through encrypted backups, ensuring compliance with data retention policies.
- **Endpoint security and threat intelligence:** Protect medical records from cyberthreats using AI-driven security solutions.
- **Incident response and recovery:** Rapid response mechanisms to mitigate breaches and ensure business continuity.

Both on-cloud and on-premises deployments are available to fit your needs in terms of control and shared responsibilities.

On cloud

The Japanese government strongly advocates for cloud adoption, as demonstrated by the establishment of the Digital Agency and the introduction of Japan's first cloud directive.

A cloud deployment with a trusted partner enables shared responsibilities while enhancing cybersecurity posture for health data protection in compliance with 2G3M requirements.

The cloud-based deployment of Acronis Cyber Protect delivers a cost-effective, easy-to-manage and comprehensive cyber protection solution for health care data.

On premises

On-premises deployment prioritizes direct control over corporate data, licensing and IT resources. It provides enhanced customization, performance and oversight, alongside comprehensive security and backup capabilities.

Acronis Cyber Protect can also be deployed in air-gapped environments, ensuring protection for systems that remain completely disconnected from the network but still require monitoring, backup and full restoration with a single click.

Acronis' cybersecurity posture

Acronis maintains a comprehensive information security and compliance program, incorporating human, organizational, physical and technical controls based on continuous risk assessments.

To ensure the effectiveness of this program, Acronis conducts ongoing monitoring, as well as internal and external audits to verify compliance with established security standards. This proactive approach enables Acronis to evaluate its security program performance and swiftly respond to emerging threats by continuous improvement.

Acronis follows a secure software development lifecycle (S-SDLC) to integrate cybersecurity considerations from the initial development stages, ensuring a security-by-design and privacy-by-design approach. Key aspects include:

- Implementation of best practices for secure design and development.
- Security and privacy design reviews using threat modeling.
- Automated static code analysis (SAST) and security bill of materials (SBOM) integrated into the CI / CD pipeline to provide real-time security feedback to developers.
- Continuous cybersecurity awareness training to foster a strong cybersecurity culture and keep teams vigilant against emerging threats.

Acronis Threat Research Unit (TRU) is a dedicated team of cybersecurity experts at Acronis that focuses on providing in-depth research and analysis of emerging cyberthreats, including malware, ransomware, phishing and advanced persistent threats (APTs). TRU publications and updates can be found at TRU Security by Acronis.

Acronis has been running a bug bounty program on HackerOne since 2018, working closely with the security community and engaging independent researchers.

As a CVE Program partner, Acronis is a CVE Numbering Authority (CNA), responsible for publishing disclosed cybersecurity vulnerabilities as CVE records for all Acronis products. For security advisories and updates, visit the Acronis Security Advisory Database.

Acronis claims compliance with 2G3M for its secure cloud services. To learn more about Acronis' compliance on this topic, visit the 2G3M page at our Trust Center.

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs) and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect Cloud is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses.

About the author

With over two decades of experience in cybersecurity, Christian Nicita (ISO 27001 LA, CCSK) is a recognized expert in cybersecurity governance, risk management, and compliance. His career spans leadership roles in top-tier organizations, where he has successfully led the implementation of international security standards, including ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018.

As a Cybersecurity Governance, Risk and Compliance Specialist at Acronis, he plays a key role in defining security policies, advancing risk mitigation strategies, conducting threat modeling, and ensuring compliance with key regulatory frameworks, including GDPR, ENS and 2G3M.

With a deep technical foundation in application security, penetration testing and secure software development, he bridges the gap between security strategy and technical execution, ensuring resilience against emerging cyberthreats. Christian has provided cybersecurity advisory services to global enterprises in telecommunications, utilities, banking and cloud services, enhancing their security posture and compliance readiness.

Appendix A: Shared Responsibility Matrix for 2G3M

The Shared Responsibility Matrix for 2G3M clarifies the distinct cybersecurity and compliance obligations of different entities handling medical data. It ensures that all stakeholders understand their roles in maintaining security and regulatory compliance.

Role	Primary Responsibilities under 2G3M
Personal Information Handling Business Operators (PIHBOs)	Establish and oversee comprehensive cybersecurity governance, risk management and compliance frameworks. Implement encryption, access controls and incident response measures to protect patient data. Ensure third-party compliance with security standards.
Entrusted Persons	Implement and enforce security controls when processing medical data on behalf of PIHBOs. Ensure compliance with data protection protocols, conduct regular security assessments and maintain a robust incident response strategy.
Subcontractors	Support cybersecurity measures by adhering to 2G3M security requirements. Implement data security controls, ensure system integrity and comply with risk management protocols established by PIHBOs and Entrusted Persons.

This matrix serves as a reference for aligning responsibilities and fostering a coordinated security approach across all entities involved in handling medical data.

Acronis

Learn more at
www.acronis.com