

---

CHAMBERS GLOBAL PRACTICE GUIDES

---


# Cybersecurity 2025

---

Definitive global law guides offering  
comparative analysis from top-ranked lawyers

**Japan: Law and Practice**

Yoshifumi Onodera, Hiroyuki Tanaka,  
Naoto Shimamura and Rio Ichii  
Mori Hamada & Matsumoto



# JAPAN



## Law and Practice

### Contributed by:

Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii  
**Mori Hamada & Matsumoto**

## Contents

### 1. General Overview of Laws and Regulators p.5

1.1 Cybersecurity Regulation Strategy p.5

1.2 Cybersecurity Laws p.5

1.3 Cybersecurity Regulators p.7

### 2. Critical Infrastructure Cybersecurity p.7

2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.7

2.2 Critical Infrastructure Cybersecurity Requirements p.8

2.3 Incident Response and Notification Obligations p.8

2.4 State Responsibilities and Obligations p.10

### 3. Financial Sector Operational Resilience Regulation p.10

3.1 Scope of Financial Sector Operational Resilience Regulation p.10

3.2 ICT Service Provider Contractual Requirements p.10

3.3 Key Operational Resilience Obligations p.11

3.4 Operational Resilience Enforcement p.11

3.5 International Data Transfers p.11

3.6 Threat-Led Penetration Testing p.12

### 4. Cyber-Resilience p.12

4.1 Cyber-Resilience Legislation p.12

4.2 Key Obligations Under Legislation p.12

### 5. Security Certification for ICT Products, Services and Processes p.12

5.1 Key Cybersecurity Certification Legislation p.12

### 6. Cybersecurity in Other Regulations p.12

6.1 Cybersecurity and Data Protection p.12

6.2 Cybersecurity and AI p.12

6.3 Cybersecurity in the Healthcare Sector p.12

**Contributed by:** Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
**Mori Hamada & Matsumoto**

**Mori Hamada & Matsumoto** is a full-service law firm that has served clients with distinction since its establishment in December 2002. Mori Hamada & Matsumoto is made up of experienced lawyers with considerable expertise in the constantly evolving and increasingly complex areas of information technology, life sciences and intellectual property, providing a variety of legal services in response to the diverse

legal needs of its clients. These legal services include advising on regulatory requirements, setting up business, corporate housekeeping, contract negotiations and dispute resolution. In terms of data protection, the firm has noted expertise in leveraging user information while protecting clients' businesses. Mori Hamada & Matsumoto's data protection team comprises approximately 130 lawyers.

## Authors



**Yoshifumi Onodera** is a partner at Mori Hamada & Matsumoto. Highly experienced in all kinds of data-related matters involving communication, media, competition, consumer and/or

information laws, he is particularly adept at delivering advice to both foreign and domestic clients on complex business structures spanning vast content and communication-related industries, including internet-related services, social networking services, games, music, movies and telecommunications. His expertise also extends to IP-related transactions, concerning licensing and dispute resolution aspects in the subsidiary fields of infringement litigation, invalidity trials, appellate litigation and arbitration, and licensing in relation to intellectual property, including patents, trademarks and copyright.



**Hiroyuki Tanaka** is a partner at Mori Hamada & Matsumoto, admitted to practise in Japan (Daini Tokyo Bar Association) and New York. Hiroyuki's practice areas are data

protection, IT and IP, and he has substantial experience advising foreign clients on Japanese data protection law. He is also familiar with global data protection regulations, including the GDPR and CCPA, and helps Japanese clients with global data protection compliance by working closely with local counsel. His practice area includes legal issues relating to AI (especially generative AI) and the protection of cybernetic avatars. He is an adjunct project professor at Keio University Graduate School of Law (2023-present).

# JAPAN LAW AND PRACTICE

---

**Contributed by:** Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
**Mori Hamada & Matsumoto**



**Naoto Shimamura** is a senior associate at Mori Hamada & Matsumoto, licensed in Japan (Daini Tokyo Bar Association), California and New York, and a lecturer at Ochanomizu

University and Japan Women's University. He uses his in-depth knowledge of computers and the internet to engage in technology-related cases, including those involving e-commerce, consumer protection, licensing, privacy, data protection, cybersecurity, defamation on the internet, intellectual property and dispute resolution. Naoto is also qualified as a Certified Information Privacy Professional/Europe (CIPP/E), a Certified Information Privacy Professional/United States (CIPP/US), and a Registered Information Security Specialist, which is recognised as the highest level of security engineering qualification in Japan.



**Rio Ichii** is a junior associate at Mori Hamada & Matsumoto, licensed in Japan (Daiichi Tokyo Bar Association). She has a broad portfolio and a wealth of experience across a number of

practice areas, including IT, intellectual property, healthcare and trade law. She has also written many articles on these topics.

---

## Mori Hamada & Matsumoto

16th Floor, Marunouchi Park Building  
2-6-1 Marunouchi  
Chiyoda-ku  
100-8222  
Tokyo  
Japan

Tel: +81 362 128 330  
Fax: +81 362 128 230  
Email: [info@morihamada.com](mailto:info@morihamada.com)  
Web: [www.morihamada.com](http://www.morihamada.com)

---

MORI HAMADA & MATSUMOTO

---

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
Mori Hamada & Matsumoto

## 1. General Overview of Laws and Regulators

### 1.1 Cybersecurity Regulation Strategy

The Basic Act on Cybersecurity is Japan's fundamental law on cybersecurity, and the Act on the Protection of Personal Information (APPI) is the country's principal data protection law.

Pursuant to the APPI, a personal data breach is subject to mandatory reporting and notification requirements – see **2.3 Incident Response and Notification Obligations**.

However, there is no general regulation imposing a mandatory reporting obligation for a cybersecurity incident that does not involve a personal data breach.

The Unfair Competition Prevention Act prohibits the infringement of trade secrets, and the Act on Prohibition on Unauthorised Computer Access outlaws unauthorised computer access. The Penal Code also includes penalties for some cybersecurity crimes. The Telecommunications Business Act requires telecommunications carriers to ensure the secrecy of communications.

Japan does not have specific regulations for secure software development.

For more details on the laws cited above and other relevant laws, see **1.2 Cybersecurity Laws**.

### 1.2 Cybersecurity Laws

The Basic Act on Cybersecurity regulates the responsibility of the national government and local governments for cybersecurity (Articles 4 and 5). It also stipulates the obligation of critical information infrastructure operators, cyberspace-related business providers, and research

institutions such as universities (Articles 6, 7 and 8) to exert efforts to ensure cybersecurity.

The APPI, Japan's principal data protection law, provides the basic principles for the government's regulatory policies and authority, as well as requirements for handling operators.

Another important law is the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (the "My Number Act"), which stipulates special rules for "my number" – a 12-digit individual number assigned to each resident of Japan.

The *kyorei*, or ordinances, enacted by local governments contain public sector obligations.

The Unfair Competition Prevention Act prohibits the infringement of trade secrets and provides for cause of actions in civil cases, such as compensation for damages and injunctive relief, as well as criminal sanctions. Information that is not protected as a trade secret may instead be protected as "data for limited provision". An unauthorised acquisition or utilisation of data for limited provision may be deemed to be unfair competition, which is subject to compensation for damages and injunctive relief but not criminal sanctions.

The Act on the Prohibition on Unauthorised Computer Access outlaws:

- the use of another person's identification code (eg, a password) to access remote computers via a telecommunications network;
- inputting information (excluding an identification code) or a command to evade access restrictions on remote computers via a telecommunications network;



Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
Mori Hamada & Matsumoto

- obtaining, supplying or storing someone else's identification code without legitimate reason (Articles 3, 4, 5 and 6); and
- phishing or creating a false impression of being the network administrator concerned and requesting identification codes (Article 7).

The Penal Code prohibits:

- the creation of false electromagnetic records that are related to rights, duties or the certification of facts (Article 161–2);
- fraud by using computers (Article 246–2);
- the destruction of electromagnetic records in use by a public office or concerning private rights or duties (Articles 258 and 259);
- the obstruction of a business by damaging its computers or electromagnetic records or causing them to operate counter to their original purpose (Article 234–2); and
- the creation, provision, acquisition or storage of a computer virus (Articles 168–2 and 168–3).

The Telecommunications Business Act requires telecommunications carriers to ensure the secrecy of communications (Article 41.6 (iii)) and to report serious breaches to the Ministry of Internal Affairs and Communications (MIC).

The Installment Sales Act requires businesses who handle credit card numbers to take necessary and appropriate measures to prevent the leakage, loss of, or damage to those credit card numbers (Article 35–16).

The Payment Services Act requires prepaid payment instrument issuers, funds transfer service providers, and virtual currency exchange service providers to take necessary and appropriate measures to prevent the leakage, loss of,

or damage to information pertaining to their respective businesses (Articles 21, 49 and 63–8).

Sector-specific regulators impose additional information security obligations on some industries including the financial and healthcare industries. For the financial sector, the Financial Services Agency (FSA) issued the Comprehensive Guidelines for the Supervision of Major Banks, which provide for cybersecurity obligations of financial institutions. For details on cybersecurity guidelines in finance, see **3. Financial Sector Operational Resilience Regulation**. As for the healthcare industry, an enforcement order on the Medical Care Act requires hospitals, clinics and birthing centres to take appropriate steps to ensure cybersecurity (Article 14.2) and an enforcement order of the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices also requests pharmacies to do the same (Article 11.2). Further, various ministries have issued other relevant guidelines:

- the Ministry of Health, Labour and Welfare (MHLW) issued the “Guidelines on Safety Management of Medical Information Systems” (last amended in May 2023);
- the Ministry of Economy, Trade and Industry (METI) and MIC jointly issued the “Safety Management Guidelines for Providers of Information Systems and Services Handling Medical Information” (last amended in July 2023);
- the MIC published comprehensive measures for the security of the internet of things (IoT) (July 2016); and
- the MIC published guidelines on the application of the Telecommunications Business Act to reports of serious accidents (volume 7, December 2023).

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
Mori Hamada & Matsumoto

## 1.3 Cybersecurity Regulators

The regulator tasked with enforcing and implementing the APPI is the Personal Information Protection Commission (PPC), which has the following powers under the APPI:

- to require private business operators who handle personal information (handling operators) to report or submit materials regarding its handling of personal information (Article 146), which the APPI defines as information about living individuals that can identify specific individuals or contains what is referred to in the APPI as an “individual identification code” (Article 2.1);
- to enter a handling operator’s offices or other places to investigate, make enquiries and check records or other documents (Article 146);
- to provide guidance or advice to a handling operator (Article 147);
- to recommend that a handling operator cease any act constituting a violation of the APPI and take other necessary measures to correct the violation (Article 148.1);
- to order a handling operator to take necessary measures to implement the PPC’s recommendation mentioned above and to rectify certain violations of the APPI (Articles 148.2 and 148.3); and
- when the PPC issues an order pursuant to Articles 148.2 and 148.3, and a handling operator violates the order, the PPC may publicly announce the violation (Article 148.4).

The National Police Agency and the Public Prosecutors Office are responsible for the criminal investigation and prosecution of cybercrimes.

As for non-regulatory government authorities that are also directly involved with cybersecurity, the Information Technology Promotion Agency

of Japan (IPA) and the National Center for Incident Readiness and Strategy for Cybersecurity (NISC) are notable. The IPA regularly publishes important guidelines and provides information on cybersecurity. The more important guidelines include the Cybersecurity Management Guidelines, guidelines for small and mid-sized companies on information security, and guidelines on preventing insider data breaches. The IPA also runs the J-CSIP, or the Initiative for Cybersecurity Information Sharing Partnership of Japan, which shares cybersecurity information of critical information infrastructure operators (ie, operators of businesses that provide infrastructure that is the foundation of people’s living conditions and economic activities, the functional failure or deterioration of which could have a highly significant impact on people). NISC is responsible for national-level cybersecurity under the Basic Act on Cybersecurity and regularly publishes updates to Japan’s Cybersecurity Strategy. For more on other regulators, refer to the previous sections in **1. General Overview of Laws and Regulators**.

## 2. Critical Infrastructure Cybersecurity

### 2.1 Scope of Critical Infrastructure Cybersecurity Regulation

The Cybersecurity Policy for Critical Infrastructure Protection defines the following 15 sectors as critical information infrastructure:

- airports;
- aviation;
- chemical industry;
- credit cards;
- electric power supply;
- financial services;
- gas supply;

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
Mori Hamada & Matsumoto

- information and communication;
- government and administration;
- logistics and shipping;
- medical;
- petroleum industry;
- ports and harbours;
- railways; and
- water supply.

The aforementioned Cybersecurity Policy also encourages critical information infrastructure operators to periodically assess their progress in implementing security measures and policies.

## 2.2 Critical Infrastructure Cybersecurity Requirements

Under the APPI, a handling operator not limited to critical infrastructure must take necessary and appropriate action for security control over the personal data that it handles, including preventing the leakage, loss or damage of or to personal data (Article 23).

The PPC is the regulator primarily responsible for the APPI and the My Number Act; it has published guidelines for the handling of personal information (the “PPC Guidelines”).

The PPC Guidelines provide examples of these handling measures, such as establishing and implementing basic policies, internal rules, and organisational, personal and technical security measures, as well as understanding of the external environment. “Understanding of the external environment” is a security measure, newly introduced by the amendments to the Guidelines, which requires a handling operator who processes personal data in a foreign country to understand the foreign country’s legal system for personal information protection and, taking into consideration that legal system, to take necessary and appropriate measures to ensure the

security of personal data. Effective from 1 April 2024, the PPC Guidelines also require a handling operator to take security control over personal information that is collected and expected to be treated as personal data so that a cyber-attacker may not intercept such information on behalf of the operator.

According to the APPI, when a handling operator allows its employees to handle personal data, it must exercise necessary and appropriate supervision over the employees to ensure security control over the personal data (Article 24). The APPI also requires a handling operator to ensure that the entity to whom it has entrusted the handling of personal data (eg, a third-party vendor) takes appropriate measures to ensure security control over the personal data (Article 25).

Under the Economic Security Promotion Act, important critical infrastructure businesses are individually designated by the competent ministry as Specified Essential Infrastructure Service Providers. They are required to take measures to reduce or eliminate risk factors among parties involved in the supply chain. Some of the requirements include establishing measures to:

- prevent unauthorised changes to specified critical facilities;
- prevent service interruptions;
- confirm any legal or contractual violations by parties involved in the supply chain; and
- prevent unintended changes by subcontractors.

## 2.3 Incident Response and Notification Obligations

The Cybersecurity Policy for Critical Infrastructure Protection provides for the reporting obligations of critical information infrastructure operators in the following instances:



Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
Mori Hamada & Matsumoto

- if there is a legal reporting requirement by law or regulation;
- if the operator has determined that an incident has had a serious impact on the lives of people or the operator's services and that information must be shared; and
- in other cases where the operator has determined that information must be shared.

## Definition of Data Security Incident, Breach or Cybersecurity Event

The APPI stipulates mandatory obligations to report data breach incidents to the PPC and to notify affected data subjects in cases where their rights and interests are likely to be infringed (Article 26). The PPC Ordinance defines a data security incident or breach as the occurrence or possible occurrence of the leakage or loss of, or damage to personal data. The details of the requirements are discussed below.

There is also a special rule for “my numbers” under the My Number Act. There is no general regulation to impose a mandatory reporting obligation for a cybersecurity incident that does not involve a personal data breach. However, there are various regulations generally mandating certain types of service providers to report an incident affecting their service to the authorities. This reporting obligation also covers cases where service failure happens as a result of a cyber-attack.

For example, under the Telecommunications Business Act, if an accident occurs and causes a suspension or deterioration of the quality of services for more than the prescribed number of hours and affects a certain number of users specified by the relevant ordinance, the telecommunications business operator must report the accident to the MIC. Furthermore, the MIC has the authority to issue orders to improve the busi-

ness practices of licensed telecommunications service providers. Another example is financial institutions; many laws regulating financial sectors oblige them to report material service failure to its authorities.

## Data Elements Covered

Breach of data security is applicable to personal data. The APPI defines personal data as personal information that is contained in a personal information database (Article 16.3), which is a collection of information (which includes personal information) that is systematically organised to enable a computer or some other means to search for particular personal information. However, this term excludes a collection of information that a Cabinet Order indicates as having little possibility of harming an individual's rights and interests considering how that collection uses personal information (Article 16.4). Examples of collections of information that are excluded from this definition include a commercially available telephone directory or a car navigation system.

The PPC Ordinance prescribes that a mandatory data breach report is required if a data breach includes personal data (excluding advanced encryption or other measures that are necessary to protect the rights and interests of the individual):

- containing “special care-required personal information”;
- that is likely to cause property damage if used inappropriately;
- that is likely to have been committed for an improper purpose (effective from 1 April 2024, personal information that is already collected or will be collected and expected to be treated as personal data is also included in this requirement); or
- of more than 1,000 individuals.

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
Mori Hamada & Matsumoto

Special care-required personal information is defined as personal information comprising a data principal's race, creed, social status, medical history, criminal record, the fact of having been a victim of a crime, or other descriptions that may be prescribed by a cabinet order as requiring special care in handling so as not to cause unfair discrimination, prejudice or other disadvantages to the data subject (Article 2.3).

## 2.4 State Responsibilities and Obligations

Governmental authorities that have specific jurisdiction over some of the 15 critical information infrastructure sectors have issued specific guidelines, described below, concerning cybersecurity.

For the healthcare industry, see **6.3 Cybersecurity in the Healthcare Sector**. For the financial industry, see **3. Financial Sector Operational Resilience Regulation**.

The Ministry of Land, Infrastructure, Transport and Tourism (MLIT) issued:

- the Safety Guidelines for Ensuring Information Security for Air Transport Operators for aviation services;
- the Safety Guidelines for Securing Information Security in the Airport Sector for airport services;
- the Safety Guidelines for Ensuring Information Security for Railway Operators for railway services; and
- the Safety Guidelines for Ensuring Information Security for the Logistics Sector for logistics services.

The MLIT also issues information security countermeasure checklists for railway service, bus

service, bus terminals, taxis, hotels, ferries, and airports and airport buildings.

The MHLW issued the Information Security Guidelines for the Water Sector for water services.

## 3. Financial Sector Operational Resilience Regulation

### 3.1 Scope of Financial Sector Operational Resilience Regulation

The FSA issued the Comprehensive Guidelines for the Supervision of Major Banks, etc. (the "Comprehensive Guidelines for SMB"), which mention cybersecurity obligations, referring to the Guidelines for Cyber Security in Finance Sector (the "Guidelines for CSFS"). The Comprehensive Guidelines for SMB further include measures regarding operational resilience. Operational resilience refers to the ability of financial institutions to continue to maintain the minimum level of their critical operations even in the event of a system failure, terrorist attack, cyber-attack, infectious disease, natural disaster or other event. The Comprehensive Guidelines for SMB specify the actions to be taken by the board of directors and the regulations of the authorities to achieve operational resilience.

### 3.2 ICT Service Provider Contractual Requirements

Not limited to the financial sector, when a handling operator entrusts personal data, it must exercise the necessary and appropriate supervision over the entrusted person to ensure security control over the entrusted personal data (Article 25 of the APPI). Handling operators shall supervise the trustees to ensure that the same levels of security control are taken as those imposed on the operators under the APPI.

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
Mori Hamada & Matsumoto

If a handling operator uses cloud services, it may not be considered as entrustment and thus, the aforesaid obligation under Article 25 of the APPI does not apply. Instead, businesses that use cloud services must still take appropriate security control over the personal data stored in cloud services as part of their own duties.

### 3.3 Key Operational Resilience Obligations

The Comprehensive Guidelines for SMB require businesses to report to the authorities when they become aware of a computer system failure or cybersecurity incident, when they are recovering from such incidents, and when they have identified the cause of an incident. Where the business detects that cyber-attack will or is highly likely to have an impact on customers or business, a report is required even if the system failure or incident does not occur. For details of the Comprehensive Guidelines, see 3.1 Scope of Financial Sector Operation Resilience Regulation.

### 3.4 Operational Resilience Enforcement

The FSA may impose administrative disposition on financial businesses that may violate or may have violated laws and regulations. Such disposition includes on-site inspections and orders to improve business operations.

### 3.5 International Data Transfers

For offshoring, there are special restrictions on the transfer of personal data to a foreign country. In principle, the APPI requires the transferor to obtain the prior consent of individuals whose personal data will be transferred to a third party located in a foreign country (Article 28). In other words, overseas transfer restrictions will apply if a foreign company transfers user data to another company outside Japan. Conversely, if a foreign company transfers user data to a company in

Japan, these overseas transfer restrictions will not apply. The overseas transfer restrictions apply even in the cases of outsourcing that are exceptions to local third-party data transfer restrictions.

The data subjects' consent to overseas data transfers is not necessary if:

- the foreign country is designated by the PPC as a country with a data protection regime with a level of protection equivalent to that of Japan (only EEA member countries and the UK have been designated to date);
- the third-party recipient has an equivalent system of data protection that meets the standards prescribed by the Ordinance issued by the PPC (the PPC Ordinance) – ie, either of the following:
  - (a) there is assurance, by appropriate and reasonable methodologies, that the recipient will treat the disclosed personal data in accordance with the spirit of the requirements on handling personal data under the APPI; or
  - (b) the recipient has been certified under an international arrangement, recognised by the PPC, regarding its system of handling personal data.

The implementation of the PPC Ordinance is set out in the PPC Guidelines, which provide that “appropriate and reasonable methodologies” include agreements between the data importer and the data exporter, or inter-group privacy rules, which ensure that the data importer will treat the disclosed personal data in accordance with the spirit of the APPI. With respect to a PPC recognised international framework, to date, the PPC Guidelines have identified only the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) as a recog-

Contributed by: Yoshifumi Onodera, Hiroyuki Tanaka, Naoto Shimamura and Rio Ichii,  
Mori Hamada & Matsumoto

nised international framework on the handling of personal data.

### 3.6 Threat-Led Penetration Testing

The Guidelines for CSFS require that threat-led penetration testing (TLPT) be carried out on a regular basis.

## 4. Cyber-Resilience

### 4.1 Cyber-Resilience Legislation

There is no uniform legislation on cyber-resilience. Specific aspects of cyber-resilience are stipulated in each of the individual regulations.

### 4.2 Key Obligations Under Legislation

Specific aspects of cyber-resilience are stipulated in each of the individual regulations.

## 5. Security Certification for ICT Products, Services and Processes

### 5.1 Key Cybersecurity Certification Legislation

The Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements provides an evaluation index for the security functions of IoT products. This system will be provided by the IPA, and applications are scheduled to begin in March 2025.

## 6. Cybersecurity in Other Regulations

### 6.1 Cybersecurity and Data Protection

Handling operators have to establish appropriate safeguards to protect personal data (Article 23 of the APPI) and have to report data breaches to the PPC and notify affected data subjects in cases where their rights and interests are likely to have been infringed (Article 26 of the APPI).

### 6.2 Cybersecurity and AI

The MIC and METI published the AI Business Guidelines for AI developers, AI service providers and AI users on 19 April 2024. These Guidelines urge businesses to invest in and implement robust security management throughout the entire AI lifecycle, including cybersecurity. They also suggest considering appropriate cyber-access controls.

### 6.3 Cybersecurity in the Healthcare Sector

The MHLW has issued the Guidelines on the Safety Management of Medical Information Systems (last amended in May 2023). While the MHLW Guidelines and an announcement issued by the MHLW on 29 October 2018 state that medical service providers should report a cybersecurity incident to the authority, no special rule has been issued for statutory data breach reporting and notifications in this regard.

The MIC and METI have jointly issued the Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information (last amended in July 2023).

---

## CHAMBERS GLOBAL PRACTICE GUIDES

---

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email [Rob.Thomson@chambers.com](mailto:Rob.Thomson@chambers.com)