Guidelines for Security Control in Handling Medical Information by Cloud Service Providers (Draft)

Comments of BSA | The Software Alliance
June 21, 2018

BSA | The Software Alliance ("BSA")¹ welcomes this opportunity to provide our comments with respect to the draft Guidelines for Security Control in Handling Medical Information by Cloud Service Providers (the "Guidelines") published by the Ministry of Internal Affairs and Communications (the "MIC").

BSA’s members are at the forefront of innovative technologies, products, and services, including cloud computing and related services that drive the global information economy and improve our daily lives. Cloud computing is and will continue to be one of the most important technologies for entities in every sector of the economy, and relevant regulations and policies should therefore support the growth of cloud services.

Robust Data Protection by Cloud and Data Localization Issue

BSA recognizes that medical information may include sensitive health data and that countries may appropriately adopt rules to ensure that privacy interests in such data are securely protected. However, mandates to store such data domestically will not advance that goal. To maximize the benefits of cloud services, including the cost-effectiveness thereof, it is essential to optimize data transfers on a global scale and to ensure smooth cross-border data transfers in a global manner. The security of electronic data depends far more on the practices of, and the technologies deployed by, the entity that stores and processes the data than on the location where such processing or storage takes place. Because leading cloud service providers ("CSPs") today implement far more robust data protection and security practices than nearly any entity could reasonably undertake on its own, the fact is that data stored in the cloud can

¹ BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world’s most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

have more up-to-date security than data stored locally, regardless of the location of the
datacenter in which the data sits. In addition, several CSPs give users, including medical
institutions, the option to select the region(s) in which their data will be stored, thereby making it
easier for medical institutions to comply with applicable data protection and other rules. The
paragraphs related to the location of information and equipment set forth in the Guidelines
appear to require the localization of data, applications, and hardware in Japan and may restrict
cross-border data transfers. The Guidelines state that these requirements are to facilitate the
ability of medical institutions to provide necessary information to the competent Japanese
authorities. Such restrictions are significantly greater than required to protect the privacy and
security of medical records and are not necessary to allow medical institutions to access and
provide necessary information upon demand. Furthermore, such requirements may dissuade
users from using cloud services. Thus, we urge the MIC to remove such paragraphs (see
Section 3 below in “Specific Comments”).

**Emphasis on International Standards**

Although the Guidelines recognize, in Section 2.4, that obtaining fair third party certification
(e.g. for information security management systems (“ISMS”)) when a CSP handles medical
information is an effective means of fulfilling a CSPs accountability toward a medical institution,
the Guidelines would benefit from more clearly and strongly emphasizing the importance of
relevant internationally recognized standards throughout the document. The draft Guidelines
could explicitly state that the requirements for CSPs in the draft Guidelines may be satisfied
and replaced by such internationally recognized standards. In addition to ISMS (ISO/IEC
27001), specific examples of such internationally recognized standards include ISO/IEC 27017
and ISO/IEC 27018. These standards have been formulated by experts and adopt an objective
review system. Certain international standards and relevant certifications ensure the service
provider’s conformity by way of audits. Using widely adopted, internationally recognized
standards and relevant certifications ensures greater security of services and provides more
confidence to medical institutions.

In addition, we recommend MIC to draft the Guidelines following the framework of, and using
terminology consistent with, such international standards. In addition to ISMS, there are several
other internationally recognized standards tailored more specifically for cloud computing that
MIC may wish to more explicitly incorporate into the Guidelines. Examples include, ISO/IEC
17788 (Cloud computing – Overview and vocabulary) and ISO/IEC 17789 (Cloud computing –
Reference architecture). Indeed, ISO/IEC 27017 directly refers to these two standards. Also,
ISO/IEC 19086-1 (Cloud computing – Service level agreement (SLA) framework – Part 1:
Overview and concepts) may be very useful for developing Cloud SLA guidelines.

**Effectiveness of High-Level Guidance rather than Prescriptive Guidelines**

We appreciate the MIC’s effort to provide guidelines to protect medical information while using
innovative cloud services. However, we would caution against imposing overly detailed and
prescriptive requirements and encourage MIC to focus more on high-level guidance. Detailed
uniform security control methods will become a burden and place a great degree of constraint
on medical institutions in their use of innovative and reliable cloud services which could be
beneficial for using, storing, and securing medical information. Further, the Guidelines fail to
thoroughly explain the difference between the public cloud and private cloud, and do not
adequately acknowledge the differences among distinct types of cloud services, such as
infrastructure-as-a-service ("IaaS"), platform-as-a-service ("PaaS"), and software-as-a-service
("SaaS"). Thus, we urge MIC to articulate that the security control requirements for CSPs
described in the Guidelines are merely for reference purposes and that many measures may
not be applicable or relevant for cloud services which medical institutions may select since the
Guidelines intend to cover various types of cloud services, and the technology and functions of
each cloud service vary.

Specific Comments Regarding the Guidelines

BSA provides the following specific comments and recommendations regarding the Guidelines
based on the basic considerations discussed above.

1. "Concept of allocation of responsibilities between CSPs and managers of medical
institutions" (Section 2.2) and "Responsibility of CSPs in managing medical information"
(Section 2.3)

As pointed out in the Guidelines, it is important to share responsibilities between medical
institutions and CSPs regarding the use of public cloud services. Further, it is necessary for
CSPs and managers of medical institutions to agree on the allocation of responsibilities.
However, such allocation of responsibilities varies greatly depending on the type of services
(e.g., IaaS, PaaS, SaaS). Since the Guidelines aim to cover a wide variety of cloud services,
they should clearly explain that the allocation of responsibilities will also vary depending on the
nature and type of services provided.

2. Security Control Requirements for CSPs (Chapter 3)

Appropriate and necessary security controls vary depending on the functions and technologies
adopted by the CSPs and the use scenarios of medical institutions. Since the Guidelines intend
to cover various types of cloud services, we encourage MIC to clearly note that the security
control requirements for CSPs described in the Guidelines are merely for reference purposes
only and that many measures may not be applicable or relevant for cloud services to be used
by medical institutions. This may help ensure medical institutions clearly understand that they
may adopt the cloud services they need without needing to comply with unreasonable or
inapplicable requirements in the draft Guidelines.
3. Page 107 in the main body of the draft Guidelines and page 17 in the example of the service
level agreement (“SLA”)

As we describe above, leading CSPs implement robust data protection and security practices,
and the security of electronic data depends far more on the practices and technologies adopted
by the CSP that stores and processes the data than on the location in which such processing or
storage takes place. Thus, we strongly urge MIC to remove the following paragraphs.

(Page 107 in the main body of Guidelines)
3.2.8 Security Control Measures for Emergency Response to Disasters
(2) Security control measures for emergency response to disasters

- The applications, platforms, server storages, etc. used to provide the services shall be
  installed in places subject to Japanese laws so that medical institutions can smoothly
  submit the materials to be submitted to the competent authorities based on the laws and
  regulations.

(Page 17 in the example of the SLA)
3.3. Prerequisites for the Environment and Operation of the Services
The storage of entrusted information and programs, and the relevant servers and
equipment for providing this service, shall be installed in places subject to the laws and
regulations of Japan.

It is not necessary to require localization of CSP hardware and entrusted data in Japan.
Medical institutions can, by contract, have real-time access to data and smoothly provide
necessary information to the competent authorities regardless of where the data and servers
may reside.

Conclusion:
BSA hopes our comments will be useful as you finalize the Guidelines, but also more generally,
we will be happy to continue to collaborate with MIC into the future. Please let us know if you
have any questions or would like to discuss these comments in more detail.

-End-