TECHNICAL REPORT

ISO/TR 21332

First edition
2021-04

Health informatics — Cloud computing considerations for the security and privacy of health information systems

Informatique de santé — Considérations relatives à l'informatique en nuage pour la sécurité et la confidentialité des systèmes d'information de santé

Reference number
ISO/TR 21332:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document identifies core Electronic Health Record (EHR) security and privacy requirements where cloud computing services are utilized. Additional requirements may also be needed where local legal or regulatory requirements exist. Potential additions or modifications can be considered by the cloud service providers in their contractual arrangements.

Cloud computing usage and adoption is becoming popular for healthcare applications worldwide. However, there are health information systems in the market that were not originally designed to operate in such an environment. The appeal and reasons for use that lead to cloud computing adoption are varied, but the available solutions do not always take into account the necessary security and privacy precautions and the necessary measures for secure use of this platform. Migration is a key consideration, as is the design of new systems to account for this type of environment.

The security and privacy of EHRs are paramount considerations for organizations that use health information systems based on cloud services, and for the patient's trust and confidence that their information is processed and stored safely and securely.

This document includes perspective of health information on cloud computing and health informatics requirements. It also provides guidance on selecting service providers in the public cloud for safely locating healthcare data, and confidential patient information (including solutions on handling of data off-shoring).

Health informatics — Cloud computing considerations for the security and privacy of health information systems

1 Scope

This document provides an overview of security and privacy considerations for Electronic Health Records (EHR) in a cloud computing service that users can leverage when selecting a service provider.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
application capabilities type
cloud capabilities type (3.2) in which the *cloud service customer* (3.8) can use the *cloud service provider's* (3.11) applications

[SOURCE: ISO/IEC 17788:2014, 3.2.1]

3.2
cloud capabilities type
classification of the functionality provided by a *cloud service* (3.5) to the *cloud service customer* (3.8), based on resources used

Note 1 to entry: The cloud capabilities types are *application capabilities type* (3.1), *infrastructure capabilities type* (3.24) and *platform capabilities type* (3.31).

[SOURCE: ISO/IEC 17788:2014, 3.2.4]

3.3
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

[SOURCE: ISO/IEC 17788:2014, 3.2.5]

3.4
cloud deployment model
way in which *cloud computing* (3.3) can be organized based on the control and sharing of physical or virtual resources

Note 1 to entry: The cloud deployment models include community cloud, hybrid cloud, private cloud and public cloud.

[SOURCE: ISO/IEC 17788:2014, 3.2.7]

3.5
cloud service
one or more capabilities offered via *cloud computing* (3.3) invoked using a defined interface

[SOURCE: ISO/IEC 17788:2014, 3.2.8]

3.6
cloud service category
group of *cloud services* (3.5) that possess some common set of qualities

Note 1 to entry: A cloud service category can include capabilities from one or more *cloud capabilities types* (3.2).

[SOURCE: ISO/IEC 17788:2014, 3.2.10]

3.7
cloud service customer data
class of data objects under the control, by legal or other reasons, of the *cloud service customer* (3.8) that were input to the *cloud service* (3.5), or resulted from exercising the capabilities of the *cloud service* (3.5) by or on behalf of the *cloud service customer* (3.8) via the published interface of the *cloud service* (3.5)

Note 1 to entry: An example of legal controls is copyright.

Note 2 to entry: It may be that the *cloud service* (3.5) contains or operates on data that is not *cloud service customer* data; this might be data made available by the *cloud service providers* (3.11), or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the *cloud service customer* (3.8) using the capabilities of the *cloud service* (3.5) on this data is likely to be *cloud service customer data* (3.7), following the general principles of copyright, unless there are specific provisions in the *cloud service* (3.5) agreement to the contrary.

[SOURCE: ISO/IEC 17788:2014, 3.2.12]

3.8
cloud service customer
CSC
party which is in a business relationship for the purpose of using *cloud services* (3.5)

Note 1 to entry: A business relationship does not necessarily imply financial agreements.

[SOURCE: ISO/IEC 17788:2014, 3.2.11]

3.9
cloud service derived data
class of data objects under *cloud service provider* (3.11) control that are derived as a result of interaction with the *cloud service* (3.5) by the *cloud service customer* (3.8)

Note 1 to entry: *Cloud service* (3.5) derived data includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the *cloud service* (3.5) has such configuration and customization capabilities.

[SOURCE: ISO/IEC 17788:2014, 3.2.13]

3.10
cloud service partner
party which is engaged in support of, or auxiliary to, activities of either the *cloud service provider* (3.11) or the *cloud service customer* (3.8), or both

[SOURCE: ISO/IEC 17788:2014, 3.2.14]

3.11
cloud service provider
party which makes *cloud services* (3.5) available

[SOURCE: ISO/IEC 17788:2014, 3.2.15]

3.12
communications as a service
CaaS
cloud service category (3.6) in which the capability provided to the *cloud service customer* (3.8) is real time interaction and collaboration

Note 1 to entry: CaaS can provide both *application capabilities type* (3.1) and *platform capabilities type* (3.31).

[SOURCE: ISO/IEC 17788:2014, 3.2.18]

3.13
community cloud
cloud deployment model (3.4) where *cloud services* (3.5) exclusively support and are shared by a specific collection of *cloud service customers* (3.8) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection

[SOURCE: ISO/IEC 17788:2014, 3.2.19]

3.14
compute as a service
CompaaS
cloud service category (3.6) in which the capabilities provided to the *cloud service customer* (3.8) are the provision and use of processing resources needed to deploy and run software

Note 1 to entry: To run some software, capabilities other than processing resources may be needed.

[SOURCE: ISO/IEC 17788:2014, 3.2.20]

3.15
cyber-incident
cyber-event that involves a loss of information security or impacts business operations

[SOURCE: ISO/IEC 27102:2019, 3.1]

3.16
cyber-insurance
insurance that covers or reduces financial loss to the insured caused by a *cyber-incident* (3.15)

[SOURCE: ISO/IEC 27102:2019, 3.2]

3.17
cyber-risk
risk caused by a *cyber-threat* (3.18)

[SOURCE: ISO/IEC 27102:2019, 3.4]

3.18
cyber-threat
threat that exploits a *cyberspace* (3.19)

[SOURCE: ISO/IEC 27102:2019, 3.5]

3.19
cyberspace
interconnected digital environment of networks, services, systems, and processes

[SOURCE: ISO/IEC 27102:2019, 3.6]

3.20
insured
entity that shares or considers sharing *cyber-risk* (3.17) with an insurer

[SOURCE: ISO/IEC 27102:2019, 3.7]

3.21
data storage as a service
DSaaS
cloud service category (3.6) in which the capability provided to the *cloud service customer* (3.8) is the provision and use of data storage and related capabilities

Note 1 to entry: DSaaS can provide any of the three *cloud capabilities types* (3.2).

[SOURCE: ISO/IEC 17788:2014, 3.2.22]

3.22
hybrid cloud
cloud deployment model (3.4) using at least two different *cloud deployment models* (3.4)

[SOURCE: ISO/IEC 17788:2014, 3.2.23]

3.23
infrastructure as a service
IaaS
cloud service category (3.6) in which the *cloud capabilities type* (3.2) provided to the *cloud service customer* (3.8) is an *infrastructure capabilities type* (3.24)

Note 1 to entry: The *cloud service customer* (3.8) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The *cloud service customer* (3.8) may also have limited ability to control certain networking components (e.g. host firewalls).

[SOURCE: ISO/IEC 17788:2014, 3.2.24]

3.24
infrastructure capabilities type
cloud capabilities type (3.2) in which the *cloud service customer* (3.8) can provision and use processing, storage or networking resources

[SOURCE: ISO/IEC 17788:2014, 3.2.25]

3.25
network as a service
NaaS
cloud service category (3.6) in which the capability provided to the *cloud service customer* (3.8) is transport connectivity and related network capabilities

Note 1 to entry: NaaS can provide any of the three *cloud capabilities types* (3.2).

[SOURCE: ISO/IEC 17788:2014, 3.2.28]

3.26
personally identifiable information
PII
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the PII principal. To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

3.27
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.26) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others (e.g. *PII processors* (3.29)) to process *PII* (3.26) on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2011, 2.10]

3.28
PII principal
natural person to whom the *personally identifiable information (PII)* (3.26) relates

Note 1 to entry: Depending on the jurisdiction and the particular *PII* (3.26) protection and privacy legislation, the synonym "data subject" can also be used instead of the term *"PII principal"* (3.28).

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.29
PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.26) on behalf of and in accordance with the instructions of a *PII controller* (3.27)

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.30
platform as a service
PaaS
cloud service category (3.6) in which the *cloud capabilities type* (3.2) provided to the *cloud service customer* (3.8) is a *platform capabilities type* (3.31)

[SOURCE: ISO/IEC 17788:2014, 3.2.30]

3.31
platform capabilities type
cloud capabilities type (3.2) in which the *cloud service customer* (3.8) can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the *cloud service provider* (3.11)

[SOURCE: ISO/IEC 17788:2014, 3.2.31]

3.32
private cloud
cloud deployment model (3.4) where *cloud services* (3.5) are used exclusively by a single *cloud service customer* (3.8) and resources are controlled by that *cloud service customer* (3.8)

[SOURCE: ISO/IEC 17788:2014, 3.2.32]

3.33
public cloud
cloud deployment model (3.4) where *cloud services* (3.5) are potentially available to any *cloud service customer* (3.8) and resources are controlled by the *cloud service provider* (3.11)

[SOURCE: ISO/IEC 17788:2014, 3.2.33]

3.34
software as a service
SaaS
cloud service category (3.6) in which the *cloud capabilities type* (3.2) provided to the *cloud service customer* (3.8) is an *application capabilities type* (3.1)

[SOURCE: ISO/IEC 17788:2014, 3.2.36]

3.35
reversibility
process for *cloud service customers* (3.8) to retrieve their *cloud service customer data* (3.7) and application artefacts and for the *cloud service provider* (3.11) to delete all *cloud service customer data* (3.7) as well as contractually specified *cloud service derived data* (3.9) after an agreed period

[SOURCE: ISO/IEC 17788:2014, 3.2.35]

4 Abbreviated terms

EHR Electronic Health Record

NHS National Health System

PHI Personal Health Information

SDO Standard Development Organizations

SIEM Security Information and Event Management

WAN Wide Area Network

5 Cloud computing

5.1 General

Cloud computing is an evolving paradigm. This is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

There are known risks to confidentiality and security using a cloud computing environment. However, the use of a cloud computing architecture over advanced technologies can produce valuable benefits. The challenge for health informatics is what deployment method to use with the available resources to maintain a trusted yet useful service.

5.2 Overview of cloud computing

This overview introduced the following.

a) **Six key cloud computing characteristics:**

i) Broad network access

It is a feature where the physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms. The focus of this key characteristic is that cloud computing offers an increased level of convenience in that users can access physical and virtual resources from wherever they need to work, as long as it is network accessible, using a wide variety of clients, including devices such as mobile phones, tablets, laptops, and workstations.

ii) Measured service

It is a feature where the metered delivery of cloud services is such that usage can be monitored, controlled, reported, and billed. This is an important feature needed to optimize and validate the delivered cloud service. The focus of this key characteristic is that the customer only pays for the resources that they use. From the customers' perspective, cloud computing offers the users value by enabling a switch from a low efficiency and asset utilization business model to a high efficiency one.

iii) Multi-tenancy

It is a feature where physical or virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from and inaccessible to one another. Typically, and within the context of multi-tenancy, the group of cloud service users that form a tenant will all belong to the same cloud service customer organization. There might be cases where the group of cloud service users involves users from multiple different cloud service customers, particularly in the case of public cloud and community cloud deployments. However, a given cloud service customer organization might have many different tenancies with a single cloud service provider representing different groups within the organization.

iv) On-demand self-service

It is a feature where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider. The focus of this key characteristic is that cloud computing offers users a relative reduction in costs, time, and effort needed to take an action, since it grants the user the ability to do what they need, when they need it, without requiring additional human user interactions or overhead.

v) Rapid elasticity and scalability

These are features where physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources. For the cloud service customer, the physical or virtual resources available for provisioning often appear to be unlimited and can be purchased in any quantity at any time automatically, subject to constraints of service agreements. Therefore, the focus of these key characteristics is that cloud computing means that the customers no longer need to worry about limited resources and might not need to worry about capacity planning.

vi) Resource pooling

It is a feature where a cloud service provider's physical or virtual resources can be aggregated in order to serve one or more cloud service customers. The focus of this key characteristic is that cloud service providers can support multi-tenancy while at the same time use abstraction to mask the complexity of the process from the customer. From the customer's perspective, all they know is that the service works, while they generally have no control or knowledge over how the resources are being provided or where the resources are located. This offloads some of the customer's original workloads such as maintenance requirements, to the provider. Even with this level of abstraction, it can be noted that users might still be able to specify location at a higher level of abstraction (e.g. country, state, or data centre).

b) **Three cloud capabilities types:**

1) Application capabilities type

2) Infrastructure capabilities type

3) Platform capabilities type

c) **An extensible set of cloud service categories including but not limited to the following:**

— Software as a Service (SaaS)

— Platform as a Service (PaaS)

— Infrastructure as a Service (IaaS)

— Network as a Service (NaaS)

— Communications as a Service (CaaS)

— Compute as a Service (CompaaS)

— Data Storage as a Service (DSaaS)

d) **Four cloud deployment models:**

1) Public cloud

2) Private cloud

3) Community cloud

4) Hybrid cloud

5.3 Cloud computing roles and activities

Within the context of cloud computing, it is often needed to differentiate requirements and issues for certain parties. These parties are entities that play roles, which set of competencies and/or performances that are associated with a task. Tasks, in turn, have sets of activities and those activities are implemented by components. All cloud computing-related activities can be categorized into three main groups: activities that use services, activities that provide services and activities that support services. It is important to note that a party can play more than one role at any given point in time and can only engage in a specific subset of activities of that role. Table 1 shows a set of roles and describes their main characteristics.

Table 1 — The major roles of cloud computing

Role	Description
Cloud service customer	The business relationship is with a cloud service provider or a cloud service partner. Key activities for a cloud service customer include, but are not limited to, using cloud services, performing business administration, and administering use of cloud services.
Cloud service partner	A cloud service partner's activities vary depending on the type of partner and their relationship with the cloud service provider and the cloud service customer. Examples of cloud service partners include cloud auditor and cloud service broker.
Cloud service provider	The cloud service provider focuses on activities necessary to provide a cloud service and activities necessary to ensure its delivery to the cloud service customer as well as cloud service maintenance. The cloud service provider includes an extensive set of activities (e.g. provide service, deploy and monitor service, manage business plan, provide audit data, etc.) as well as numerous sub-roles (e.g. business manager, service manager, network provider, security and risk manager, etc.).

5.4 Cloud capabilities types and cloud service categories

A cloud capabilities type is a classification of the functionality provided by a cloud service to the cloud service customer, based on the resources used. There are three different cloud capabilities types:

a) application capabilities type;

b) infrastructure capabilities type;

c) platform capabilities type.

These are different because they follow the principle of separation of concerns, i.e. they have minimal functionality overlap between each other.

Table 2 describes the cloud capabilities.

Table 2 — Cloud capability types

Cloud capability type	Description
Application capabilities	The cloud service customer can use the cloud service provider's applications.
Infrastructure capabilities	The cloud service customer can provision and use processing, storage, or networking resources
Platform capabilities	The cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider.

The cloud capabilities types should not be confused with other categorizations of cloud services.

A cloud service category is a group of cloud services that possess some common set of qualities. A cloud service category can include capabilities from one or more cloud capabilities types. Representative cloud service categories can be found in Table 3.

Table 3 — Cloud service categories

Cloud service categories	Description
Communications as a Service (CaaS):	A cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration.
Compute as a Service (CompaaS)	A cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software.
Data Storage as a Service (DSaaS)	A cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities.
Infrastructure as a Service (IaaS)	A cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.
Network as a Service (NaaS)	A cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.
Platform as a Service (PaaS)	A cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.
Software as a Service (SaaS)	A cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

It is expected that there will be additional cloud service categories (see Annex A). This document does not imply that one cloud service category is more important than another.

5.5 Cloud deployment models

Cloud deployment models represent how cloud computing can be organized based on the control and sharing of physical or virtual resources. The cloud deployment models include several approaches, including public, private, community, and hybrid cloud.

A Public cloud a deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider. A public cloud can be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud service provider. Actual availability for specific cloud service customers can be subject to jurisdictional regulations. Public clouds have broad boundaries, where cloud service customer access to public cloud services has few, if any, restrictions.

A Private cloud is a deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer. A private cloud can be

owned, managed, and operated by the organization itself or a third party and might exist on premises or off premises. The cloud service customer can also authorize access to other parties for its benefit. Private clouds seek to set a narrowly controlled boundary around the private cloud based on limiting the customers to a single organization.

A Community cloud is a deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection. A community cloud can be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it might exist on or off premises. Community clouds limit participation to a group of cloud service customers who have a shared set of concerns, in contrast to the openness of public clouds, while community clouds have broader participation than private clouds. These shared concerns include, but are not limited to, mission, information security requirements, policy, and compliance considerations.

A Hybrid cloud is a deployment model using at least two different cloud deployment models. The deployments involved remain unique entities but are bound together by appropriate technology that enables interoperability, data portability and application portability. A hybrid cloud can be owned, managed, and operated by the organization itself or a third party and might exist on premises or off premises. A hybrid cloud is a cloud deployment model using at least two different cloud deployment models. In practice, it can be a composition of two or more clouds that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability.

These cloud deployment models are represented in Figure 1.

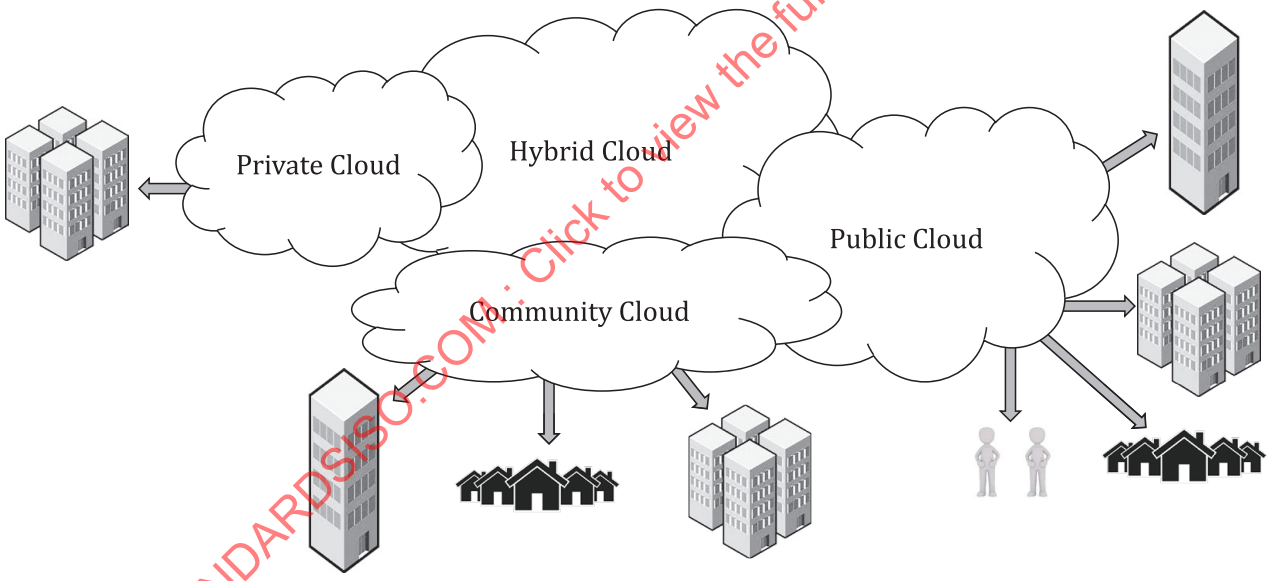


Figure 1 — Cloud deployment models

The relationship among service and deployment models can vary accordingly with availability, requirements and regional regulations. Figure 2 shows an example of the different models.

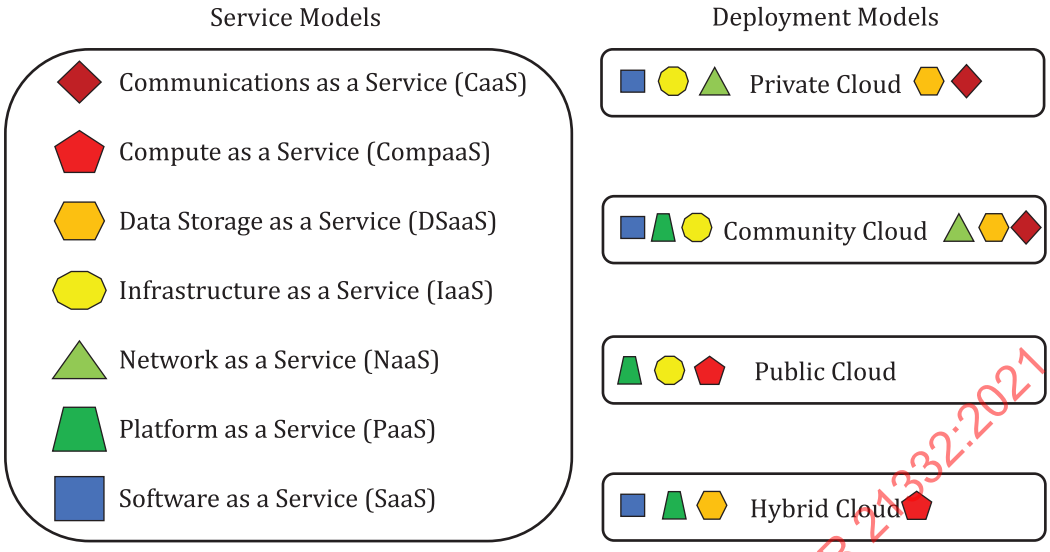


Figure 2 — Service models and deployment models example relationship

5.6 Cloud computing information system security capabilities

Behaviours or capabilities need to be coordinated across roles and implemented consistently in a cloud computing system. Such aspects may impact multiple roles, activities, and components, in such a way that it is not possible to clearly assign them to individual roles or components. These become cross-cutting aspects across the roles, activities and components.

Key cross-cutting aspects are outlined in Table 4.

Table 4 — Cross-cutting aspects

Cross-cutting aspect	Description
Auditability	The capability of collecting and making available necessary evidential information related to the operation and use of a cloud service, for the purpose of conducting an audit.
Availability	The property of being accessible and usable upon demand by an authorized entity. The "authorized entity" is typically a cloud service customer.
Governance	The system by which the provision and use of cloud services are directed and controlled. Cloud governance is cited as a cross-cutting aspect because of the requirement for transparency and the need to rationalize governance practices with SLAs and other contractual elements of the cloud service customer to cloud service provider relationship. The term "Internal cloud governance" is used for the application of design-time and run-time policies to ensure that cloud computing-based solutions are designed and implemented, and cloud computing-based services are delivered, according to specified expectations. The term "external cloud governance" is used for some form of agreement between the cloud service customer and the cloud service provider concerning the use of cloud services by the cloud service customer.
Interoperability	Ability of a cloud service customer to interact with a cloud service and exchange information according to a prescribed method and obtain predictable results.
Maintenance and versioning	Maintenance refers to changes to a cloud service or the resources it uses in order to fix faults or in order to upgrade or extend capabilities for business reasons. Versioning implies the appropriate labelling of a service so that it is clear to the cloud service customer that a particular version is in use.
Performance	A set of behaviours relating to the operation of a cloud service, and having metrics defined in an SLA.

Table 4 *(continued)*

Cross-cutting aspect	Description
Portability	Ability of cloud service customers to move their data or their applications between multiple cloud service providers at low cost and with minimal disruption. The amount of cost and disruption that is acceptable may vary based upon the type of cloud service that is being used.
Protection of PII	Protect the assured, proper, and consistent collection, processing, communication, use and disposal of Personally Identifiable Information (PII) in relation to cloud services.
Regulatory	There are a number of different regulations that can influence the use and delivery of cloud services. Statutory, regulatory, and legal requirements vary by market sector and jurisdiction, and they can change the responsibilities of both cloud service customers and cloud service providers. Compliance with such requirements is often related to governance and risk management activities.
Resilience	Ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation.
Reversibility	A process for the cloud service customer to retrieve their cloud service customer data and application artefacts and for the cloud service provider to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed period.
Security	Ranges from physical security to application security, and includes requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, non-repudiation, audit, security monitoring, incident response, and security policy management.
Service levels and service level agreement	The cloud computing service level agreement (cloud SLA) is a service level agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing specific terms to set the quality of the cloud services delivered. It characterizes quality of the cloud services delivered in terms of: 1) a set of measurable properties specific to cloud computing (business and technical) and 2) a given set of cloud computing roles (cloud service customer and cloud service provider and related sub-roles).

Many of these cross-cutting aspects, when combined with the key characteristics of cloud computing, represent good reasons for using cloud computing. However, cross-cutting aspects like security, protection of PII, and governance have been identified as major concerns and in some cases an impediment to the adoption of cloud computing.

6 Considerations for health information in cloud computing environment

6.1 Overview

At the highest level, organizations can define an “information security policy” which is approved by management and which sets out the organization’s approach to managing its information security objectives even when the information is not hosted onsite.

Information security policies can address requirements created by

a) business strategy,

b) regulations, legislation, and contracts,

c) the current and projected information security threat environment, and

d) the context sensible health information systems.

The information security policy can contain statements concerning

a) definition of information security, objectives and principles to guide all activities relating to information security,

b) assignment of general and specific responsibilities for information security management to defined roles, and

c) processes for handling deviations and exceptions.

At a foundational level, the information security policy can be supported by topic-specific policies on health context, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics.

Examples of policy topics are outlined in Annex B. Other examples to be considered are

a) access control,

b) information classification (and handling),

c) physical and environmental security,

d) end user-oriented topics such as

   1) acceptable use of assets,

   2) clear desk and clear screen,

   3) information transfer,

   4) mobile devices and teleworking, and

   5) restrictions on software installations and use.

e) backup,

f) information transfer,

g) protection from malware,

h) management of technical vulnerabilities,

i) cryptographic controls,

j) communications security,

k) privacy and protection of personally identifiable information, and

l) supplier relationships.

These policies can be communicated to employees and relevant external parties in a form that is relevant, accessible, and understandable to the intended reader, e.g. in the context of an information security awareness, education, and training program.

The need for internal policies for information security varies across organizations. Internal policies are especially useful in larger and more complex organizations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organization. Policies for information security can be issued in a single information security policy document or as a set of individual but related documents. If any of the information security policies are distributed outside the organization, care should be taken not to disclose confidential information. Some organizations use other terms for these policy documents, such as “Standards”, “Directives” or “Rules.” A policy and supporting security measures can also be implemented to protect information accessed, processed, or stored at teleworking sites such as telemedicine.

6.2 Health information security

6.2.1 Overview of Teleworking Policies and Procedures

Teleworking refers to all forms of work outside of the office, hospital, clinic and elsewhere, including non-traditional work environments, such as those referred to as “telecommuting”, “flexible workplace”, “remote work” and “virtual work” environments.

Organizations, especially those allowing teleworking activities, can issue a policy that defines the conditions and restrictions for using teleworking as an overall good practice for security regardless of location. Where deemed applicable and allowed by law, the following matters can be considered:

a) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

b) the proposed physical teleworking environment;

c) the communications security requirements, taking into account the need for remote access to the organization’s internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system;

d) the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment;

e) the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;

f) the use of home networks and requirements or restrictions on the configuration of wireless network services;

g) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

h) access to privately owned equipment (to verify the security of the machine or during an investigation), which can be prevented by legislation;

i) software licensing agreements that are such that organizations might become liable for the licensing of client software on workstations owned privately by employees or external party users;

j) malware protection and firewall requirements.

The guidelines and arrangements to consider can include the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately-owned equipment that is not under the control of the organization is not allowed. A definition of the work permitted in important element, including the hours of work, the classification of information that can be held and the internal systems and services that the teleworker is authorized to access. Other provisions to consider include physical security, hardware and software support and maintenance, audit and security monitoring, insurance, and suitable communication equipment such as methods for securing remote access. Access can also be controlled, including revocation of authority and access rights, the return of equipment when the teleworking activities are terminated, and as well as rules and guidance on family and visitor access to equipment and information. Procedures for backup and business continuity are put in place to ensure that those teleworking employees are protected against data loss and interruption. Observation of national, local privacy and access legislation that applies and stablish definitions on how/where to access can be included in all teleworking provisions.

6.2.2 Telework and portable devices

Despite its flexibility and convenience, teleworking and portable devices will bring additional risks that can be considered by the users and service providers. Using business equipment outside the organization´s IT security perimeters brings the attention to both the equipment and network connection used, and can become threats not only to confidentiality, integrity and availability of

information, but also to the safety of patients. It could result in unauthorized and undesired access to sensitive information.

The use of private portable devices also brings risks that can be considered. The BYOD (Bring Your Own Device) policy of the organization should also be followed. However, the IT security policies can consider the vulnerabilities present on different applications and systems installed, the possible lack of security applications, parameters and configurations, and the possible existing malware on such devices. The BYOD devices might have access to EHR and therefore might represent a security, confidentiality and/or patient safety breach.

Establishing certain precautions can help the use of such technology to became more secure once when it is associated to cloud services. Most of the precautions are related to equipment use policies, such as restriction of use to the employee, locking physically and by password, keep operating system and anti-malware updated, prevent the use of USB use, and avoiding the installation of unauthorized software.

However, there are some safeguards related to IT systems that are directly complementary to cloud environment security measures. Regular monitoring and maintenance of devices and network activities, the use of firewalls and anti-malware at the datacentre level, use of strong user identification and authentication, and use of updated operating system and security software are some of the important practices to be evaluated from cloud service providers.

6.3 Information security policies

6.3.1 Overview

The information security policies can be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers).

Contractual agreements can clearly allocate responsibilities between the public cloud PII processor, its sub-contractors and the cloud service customer, taking into account the type of cloud service in question (e.g. a service of an IaaS, PaaS or SaaS category of the cloud computing reference architecture). For example, the allocation of responsibility for application layer controls may differ depending on whether the public cloud PII processor is providing a SaaS service or rather is providing a PaaS or IaaS service upon which the cloud service customer can build or layer its own applications.

In some jurisdictions the public cloud PII processor is directly subject to PII protection legislation. Elsewhere, PII protection legislation applies to the PII controller only.

A mechanism to ensure the public cloud PII processor is obliged to support and manage compliance is provided by the contract between the cloud service customer and the public cloud PII processor. The contract could call for independently audited compliance, acceptable to the cloud service customer using industry standards and best practices.

6.3.2 Information security and protection of PII and PHI

The rate of data breach has grown consistently over the last 10 years[1)]. According research and surveys, PHI has more value to criminals than PII due to its continuity of value through time. PII can be cancelled or change, therefore losing its value quickly. For example, a credit card number can be expired and changed but PHI remains constant and is difficult to modify or cancel like a credit card. Credit card information and PII, while valuable assets on the black market, are not as valuable as PHI which can sell for much more.

1) Source of some statistics about data breach, especially in health organizations https://www.hipaajournal.com/healthcare-data-breach-statistics/) https://www.techrepublic.com/article/why-70-of-healthcare-orgs-have-suffered-data-breaches/) (Business insider https://www.businessinsider.com/why-healthcare-data-breach-epidemic-will-intensify-2019-4) (Healthcare IT News https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far)

The path towards cloud environment seems to be a challenge. The recommended way to face it is through the identification of Privacy and Security safeguards dedicated to protection of PII and PHI, including harmonization of the standards and industry best practice, such as the COBIT 5 Cloud Assurance and Cloud Security Alliance Cloud Control Matrix[2)].

6.3.3 Availability

Availability embodies the concept of anywhere and anytime access to services, tools, and data. Availability is also related to reliability. It is important to consider multiple redundant resources to maintain the cloud computing service, including energy sources for the data centre and even replication between multiple geographical locations in case of disasters. It also requires the selection of redundant services in order to grant access to the information, regardless of which of the infrastructure is part of the cloud computing service. Examples of restrictions to data upload and access could be related to

a) government restrictions e.g. preventing sensitive data to be stored outside the country,

b) local (Intranet) – due to antivirus programs and firewalls, or

c) service provider restrictions.

These need to be individually tested and catered to at all levels.

Services such as infrastructure-as-a-service and platform-as-a-service providers are possible for most cloud-based service providers, especially for software-based services, as well as to offer service level agreements that could provide the right level of service required for an Electronic Health Record service.

The interaction of multiple components and automated systems over distributed networks and data centres can result in issues that take a long time to be resolved. Regardless of the quality of a service provider, of their underlying hardware or platform, the chance of failure increases with complexity. A key issue is the critical dependency on the WAN links between a hospital or other healthcare premises and the data centre hosting the cloud services. These aspects can be considered within both pre-contract and routine risk assessment and options for sustainable mitigation. It can be noted that in many countries power supply reliability, broadband and other WAN services are not always considered to be satisfactory.

More important in the context of the document is the issue of availability. The service levels that a cloud provider can achieve are not the same as the service levels that a healthcare organization such as a hospital will receive. This is because the organization is dependent on the availability not only of the cloud provider's services but also of the WAN links.

If the service offered does not achieve the availability requirements, an alternative would be to replicate servers on geographically distinct locations. Services can be hosted and replicated to multiple providers, at multiple locations, to reduce the chances of failure. Even downtime related to maintenance can be reduced by spreading a service over multiple providers: the chance of planned maintenance windows overlapping between providers is small.

Artificial Intelligence (AI) techniques to provide coordinated security defences and availability can be considered as a valuable resource for cloud environment because it can be set to evaluate multiple parameters. It is recommended to evaluate which AI capabilities are offered and how can they be used to provide the required availability and security protection to EHR systems in cloud.

As it is not possible to maintain uninterrupted availability, there are some questions to ask service providers that would help understand, to some extent, the consequences of a cloud computing service unavailability: (a) What happens when the services fail? (b) Is the service provider capable of delivering on the promised availability level? (c) What is the service provider's track record?

2) Suggested source of COBIT information (http://www.isaca.org/cobit/pages/default.aspx) and Cloud Control Matrix (https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/)

6.3.4 Cloud deployment models considerations

Cloud deployment models represent how cloud computing can be organized based on the control and sharing of physical or virtual resources. The cloud deployment models include: Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud. Public clouds have broad boundaries, where cloud service customer access to public cloud services has few, if any, restrictions. Private clouds seek to set a narrowly controlled boundary around the private cloud based on limiting the customers to a single organization. Community clouds limit participation to a group of cloud service customers who have a shared set of concerns, in contrast to the openness of public clouds. Community clouds have broader participation than private clouds. These shared concerns include, but are not limited to, mission, information security requirements, policy, and compliance considerations. Hybrid clouds represent situations where interactions between two different deployments might be needed but remained linked via appropriate technologies. As such, the boundaries set by a hybrid cloud reflect its two base deployments.

Security in cloud computing can be strategically implemented regardless of deployment models, cloud capabilities types and cloud service categories. Private cloud model and a closed model that a Cloud Service provider exclusively segregates services for the Cloud Service Customer from other users can provide a Cloud Service Customer greater control over security, assurance over data location, removal of multiple jurisdiction legal and compliance requirements. Security considerations increase when adding more systems or deployment models.

When selecting cloud deployment models that best meet the requirements of protecting sensitive health data, it is necessary to understand the limitation, risk exposure and security vulnerability of each model. For example, public cloud or hybrid cloud that include public cloud would require specific constraints regarding cloud service customer data and cloud service customer derived data. There can be a special policy to rule the reversibility process available in order to grant the correct use of data or derived data, the confidentiality and security of the health records.

6.3.5 Audit trail and logs

A process can be put in place to review event logs with a specified, documented periodicity to identify irregularities and propose remediation efforts. It is important to consider a SIEM that offers the flexibility needed to deploy over complex digital environments, and the sophistication to effectively manage a wide range of threats. Indeed, SIEM tools collect, store, and analyse security information from across your organization to alert IT professionals to ongoing attacks and analyse log data to identify irregularities.

Where possible, event logs can record whether PII or other critical data has been changed (added, modified or deleted) as a result of an event and by whom. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, roles in implementing this guidance may be shared. The public cloud PII processor can define criteria regarding if, when, and how log information can be made available to or usable by the cloud service customer. These procedures can be made available to the cloud service customer.

Where a cloud service customer is permitted to access log records controlled by the public cloud PII processor, the public cloud PII processor can ensure that the cloud service customer can only access records that relate to that cloud service customer's activities, and cannot access any log records which relate to the activities of other cloud service customers. Log information recorded for purposes such as security monitoring and operational diagnostics may contain PII. Measures, such as controlling access, can be put in place to ensure that logged information is only used for its intended purposes. A procedure, preferably automatic, can be put in place to ensure that logged information is deleted within a specified and documented period.

6.3.6 Cryptography and obfuscation

When developing a cryptographic policy, the following can be considered:

a) The management approach towards the use of cryptographic controls across the organization, including the general principles under which business information can be protected.

b) Based on a risk assessment, the required level of protection can be identified considering the type, strength and quality of the encryption algorithm required.

c) The use of encryption for protection of information transported by mobile or removable media devices or across communication lines.

d) The approach to key management can include methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys.

e) Define roles and responsibilities, e.g. who is responsible for

   1) the implementation of the policy, and

   2) the key management, including key generation.

f) The standards to adopt for effective implementation throughout the organization (what solution is used for which business process) can be defined.

g) The impact of using encrypted information on controls that rely upon content inspection such as malware detection can be documented.

When implementing the organization's cryptographic policy, consideration can be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of cross-border flow of encrypted information.

Cryptographic controls can be used to achieve different information security objectives including

a) **confidentiality:** using encryption of information to protect sensitive or critical information, either stored or transmitted,

b) **integrity/authenticity:** using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information,

c) **non-repudiation:** using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action, and

d) **authentication:** using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities, and resources.

Deciding whether a cryptographic solution is appropriate can be part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control can be applied, and for what purpose and business processes. A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use. Specialist advice can be sought in selecting appropriate cryptographic controls to meet the information security policy objectives.

The public cloud PII processor can provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The public cloud PII processor can also provide information to the cloud service customer about any capabilities it provides that may assist the cloud service customer in applying its own cryptographic protection. PII that is transmitted over public data-transmission networks can be encrypted prior to transmission. In some cases, e.g. the exchange of e-mail, the inherent characteristics of public data-transmission network systems might require that some header or traffic data be exposed for effective transmission. Where

multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there may be varied or shared roles in implementation.

6.3.7 Retention, backup, and deletion

Information processing systems based on the cloud computing model introduce additional or alternative mechanisms to off-site backups for protecting against loss of data, ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a disruptive event. Multiple copies of data in physically or logically diverse locations can be created or maintained for the purposes of backup and recovery. PII-specific responsibilities in this respect may lie with the cloud service customer. Where the public cloud PII processor explicitly provides backup and restore services to the cloud service customer, the public cloud PII processor can provide clear information to the cloud service customer about the capabilities of the cloud service with respect to backup and restoration of the cloud service customer data.

NOTE 1 Individual jurisdictions can impose specific requirements regarding the frequency of backups. Organizations operating in these jurisdictions can ensure that they comply with these requirements.

Procedures can be put in place to allow for restoration of data processing operations within a specified, documented period after a disruptive event. The back-up and recovery procedures can be reviewed at a specified, documented frequency.

NOTE 2 Individual jurisdictions can impose specific requirements regarding the frequency of reviews of backup and recovery procedures. Organizations operating in these jurisdictions can ensure that they comply with these requirements.

The use of sub-contractors to store replicated or backup copies of data being processed is covered by the set of controls described in this document and apply to sub-contracted PII processing. These controls also apply where physical media transfers take place.

The public cloud PII processor can have a policy that addresses the requirements for backup of information and any further requirements, such as contractual and/or legal requirements, for the erasure of PII contained in information held for backup purposes.

6.3.8 Access control and multi-client segmentation

6.3.8.1 General

Asset owners can determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the level of detail and the strictness of the controls reflecting the associated information security risks. Access controls are both logical and physical and these can be considered together.

Users and service providers can be given a clear statement of the business requirements to be met by access controls.

The policy can take account of the following:

a) security requirements of business applications;

b) policies for information dissemination and authorization, such as the need-to-know principle and information security levels and classification of information;

c) consistency between the access rights and information classification policies of systems and networks;

d) relevant legislation and any contractual obligations regarding limitation of access to data or services,

e) management of access rights in a distributed and networked environment that recognizes all types of connections available;

f) segregation of access control roles, such as access request, access authorization, access administration;

g) requirements for formal authorization of access requests;

h) requirements for periodic review of access rights;

i) removal of access rights;

j) archiving of records of all significant events concerning the use and management of user identities and secret authentication information;

k) roles with privileged access.

Care can be taken when specifying access control rules to consider

a) establishing rules based on the premise "Everything is generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden",

b) changes in information labels that are initiated automatically by information processing facilities and those initiated at the discretion of a user,

c) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator, and

d) rules which require specific approval before enactment and those which do not.

Access control rules can be supported by formal procedures and defined responsibilities.

Role based access control is an approach used successfully by many organizations to link access rights with business roles.

Two of the frequent principles directing the access control policy are the following:

a) **Need-to-know:** you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile);

b) **Need-to-use:** you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

6.3.8.2 Assets and performance control

An organization can identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information can include creation, processing, storage, transmission, deletion and destruction. Documentation can be maintained in dedicated or existing inventories as appropriate.

The asset inventory can be accurate, up to date, consistent and aligned with other inventories.

For each of the identified assets, ownership of the asset can be assigned, and the classification can be identified. Inventories of assets help to ensure that effective protection takes place, and can also be required for other purposes, such as health and safety, insurance or financial (asset management) reasons.

ISO/IEC 27005 provides examples of assets that might need to be considered by the organization when identifying assets. The process of compiling an inventory of assets is an important prerequisite of risk management (see also ISO/IEC 27000 and ISO/IEC 27005), likewise for the purchase of cyber-insurance as a risk treatment option to share cyber-risks. ISO/IEC 27102 provides guidelines when considering purchasing cyber-insurance.

6.3.8.3 Legal and accountability

The public cloud PII processor can promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure, or alteration of PII. A SIEM would be an important tool to manage and support legal and accountability issues. Provisions covering the notification of a data breach involving PII can form part of the contract between the public cloud PII processor and the cloud service customer. The contract can specify how the public cloud PII processor will provide the information necessary for the cloud service customer to fulfil his obligation to notify relevant authorities. This notification obligation does not extend to a data breach caused by the cloud service customer or PII principal or within system components for which they are responsible. The contract can also define the maximum delay in notification of a data breach involving PII.

In the event that a data breach involving PII has occurred, a record can be maintained with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, the steps taken to resolve the incident (including the person in charge and the data recovered) and whether the incident resulted in loss, disclosure or alteration of PII. It is also important to consider what type of breach, for example human-accidental, technical, human-malicious. This will allow for better tracking and information for future planning, education, training, research.

In the event that a data breach involving PII has occurred, the record can also include a description of the data compromised, if known; and if notifications were performed, the steps taken to notify the cloud service customer and/or regulatory agencies.

In some jurisdictions, relevant legislation or regulations can require the public cloud PII processor to directly notify appropriate regulatory authorities (e.g. a PII protection authority) of a data breach involving PII.

NOTE There might be other breaches requiring notification that are not covered here, such as collection without consent or other authorization, use for unauthorized purposes, etc.

6.3.9 Change management

An organization can determine whether the continuity of information security is captured within the business continuity management process. Information security requirements can be determined when planning for business continuity. In the absence of formal business continuity planning, information security management can assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organization could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

An organization can ensure that

a) an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence,

b) incident response personnel with the necessary responsibility, authority, and competence to manage an incident and maintain information security are nominated, and

c) documented response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.

6.3.10 Disaster recovery

An organization can determine whether the continuity of information security is within the disaster recovery management process. Information security requirements can be determined when planning for disaster recovery and alternative processing sites can be addressed as part of the cloud environment and incident management/disaster recovery/business continuity planning.

In the absence of disaster recovery planning, information security management can assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an organization could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

According to the information security continuity requirements, the organization can establish, document, implement and maintain:

a) information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;

b) processes, procedures and implementation changes to maintain existing information security controls during an adverse situation;

c) compensating controls for information security controls that cannot be maintained during an adverse situation.

6.3.11 Testing and evaluation

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests can initially be performed by the development team. Independent acceptance testing can then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected. The extent of testing can be in proportion to the importance and nature of the system.

The use of operational data containing PII or any other confidential information for testing purposes can be avoided. If PII or otherwise confidential information is used for testing purposes, all sensitive details and content can be protected by removal or modification (see ISO/IEC 29101).

The following guidelines can be applied to protect operational data, when used for testing purposes:

a) the access control procedures, which apply to operational application systems, can also apply to test application systems;

b) there can be separate authorization each time operational information is copied to a test environment;

c) operational information can be erased from a test environment immediately after the testing is complete;

d) the copying and use of operational information can be logged to provide an audit trail, and intended users test setting can consider an appropriate environment, taking into account the correct user profile and access control, in order to grant more efficient and correct evaluation of the new and updates systems.

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data.

6.3.12 Information management

There is a multi-tier recommendation for Software Asset Management (SAM) available in the ISO/IEC 19770 series. This demonstrates how important it is to know the type of data and systems used by an organization to ensure proper management. The first six parts of the standard are of interest to this document and are distributed as following: ISO/IEC 19770-1 defines requirements for asset management systems. ISO/IEC 19770-2 defines the software identification tag. ISO/IEC 19770-3 defines the entitlement schema. ISO/IEC 19770-4 defines resource utilization measurement. ISO/IEC 19770-5 establishes an overview and vocabulary. ISO/IEC 19770-6[3)] is about hardware schema. ISO/IEC 19770-8

3) Under preparation. Stage at the time of publication: ISO/IEC/CD 19770-6:2020.

is also of interest. ISO/IEC 19770-11[4] establishes requirements for bodies providing audit and certification of IT asset management systems.

To better understand the proposed tiered SAM, the following provides a description and outlines each tier's benefits.

Tier 1: Trustworthy Data. To achieve this tier, the organization has foundational understanding of what is contained and can manage it.

> Good data is a prerequisite for good SAM. A common management observation which applies here is that "you cannot manage what you do not know." This tier also provides the basis for demonstrating license compliance, which is typically a high priority management objective.

Tier 2: Practical Management. To achieve this tier, an organization can improve management controls and drive immediate benefits.

> In practice, management typically only starts to take ownership of issues related to SAM after the organization has recognized the issues which result from not having trustworthy data. The organization recognizes the extent of the risks it faces as well as the opportunities for improvement and savings. This tier covers the basic management control environment (see ISO/IEC 19770-1:2017, 4.2), including policies, roles and responsibilities. It also includes targeting and delivering "quick wins" made obvious by the data of Tier 1.

Tier 3: Operational Integration. Achieving this tier results in improved efficiency and effectiveness.

> Building on the foundation of the previous two tiers, this tier drives the integration of SAM into operational processes (see ISO/IEC 19770-1:2017, 4.6). The result is improved efficiency and effectiveness.

Tier 4: Full ISO/IEC SAM conformance. Achieving this tier results in achieving best-in-class strategic SAM.

> This tier addresses the more advanced and demanding aspects of full SAM, including its full integration into strategic planning for the organization.

4) Under preparation. Stage at the time of publication: ISO/IEC/PRF 19770-11:2021.

Annex A
(informative)

Example guidance from the UK for selecting and risk managing cloud based digital health services

A.1 Guidance and recommendations for selecting

A.1.1 General

This annex is based on a jointly published paper by the Department of Health and Social Care, NHS England, NHS Digital[10] and NHS Improvement. According to it, the NHS and social care organizations can safely locate health and care data, including confidential patient information, in the public cloud, including solutions that make use of data off-shoring. The paper provides advice and guidance regarding the safeguards that should be put in place to do so.

This document explains the process and provides details on what proportionate controls should be put in place.

A.1.2 Overview

It is a process that involves four recommendations. It should be used at the start of any digital project to understand the risk of the data that needs to be stored and processed and the safeguards that can be put in place to do so. The recommendation are as follows:

— Recommendation 1 – Understand the data you are dealing with.

— Recommendation 2 – Assess the risks associated with the data.

— Recommendation 3 – Implement appropriate controls.

— Recommendation 4 – Monitor the implementation and ongoing risks.

A.2 Recommendations

A.2.1 Recommendation 1 – Understand

The first step is to understand the data that will be handled. This can include the following:

a) List all the data fields/attributes that will be stored or processed by the system.

b) Quantify how much data is under consideration.

c) Consider how long the data will be held in the system.

d) Understand the Service Classification (see Annex C) of the system (Bronze | Silver | Gold | Platinum). This relates to the availability SLAs and will be used to determine the cloud security approach for availability and integrity. The service classification is normally agreed between the owning Programme and Service management.

e) Carefully assess the data fields/attributes and decide which Data Type(s) this relates to.

f) Based on this information, use the NHS Digital Data Risk Model to calculate the risk classification of the data.

g) Ensure to document the outputs of the above, specifically:

1) Retain the list of data types/attributes.

2) Record the rationale for selecting the data type(s).

3) Retain the completed risk model.

The risk classification is used to help you understand the following:

— The risk profile and the associated governance that we would expect you to undertake.

— The controls that are needed to be put in place to mitigate the risk.

A.2.2 Recommendation 2 – Assess

A.2.2.1 General

This step is about assessing the risk and identifying governance requirements for putting the data in the cloud. At the end of this step, users should have decided on whether to use public cloud to host their system.

A.2.2.2 Risk Appetite

Different organization and programmes will have different appetites towards risk and this appetite may vary over time.

— Class I defines the lowest level of risk.

— Class V defines the highest level of risk.

However, proportionate controls are available to help mitigate these risks, regardless of whether the risk is classified as Class I or Class V. These are detailed in Recommendation 3 (see A.2.3). It is important to understand your organization's risk appetite, implement controls and monitor their effectiveness as part of your ongoing governance process.

A.2.2.3 Governance

Using the Risk Classification obtained in Recommendation 1 (see A.2.1), see Table A.1 for examples of governance expectations.

Table A.1 — Risks Profile Levels

Risk Profile Level	Expectation
Class I	All organizations are expected to be comfortable operating services at this level.
Class II	Whilst there may be some concerns over public perception and lock-in, most organizations are expected to be comfortable operating services at this level.
Class III	At this level, risks associated with impact of breach become more significant, and the use of services at this level therefore requires specific risk management across all risk classes described in Part 4 of Reference [26], requiring approval by CIO / Caldicott Guardian [a] level.
Class IV	At this level, it may become more difficult to justify that the benefits of the using public cloud outweigh the risks. However, a case may still be made, requiring approval by CIO / Caldicott Guardian, and be made visible to the organization's Board. Specialist advice and guidance should be sought.
Class V	Operating services at this level would require board-level organizational commitment, following specialist advice and guidance.

[a] A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. https://www.gov.uk/government/groups/uk-caldicott-guardian-council

A.2.2.4 Other considerations

A.2.2.4.1 General

Security is not the only aspect that you should consider when moving to cloud. Other elements to think about are listed in A.2.2.4.2 to A.2.2.4.8.

A.2.2.4.2 Public perception

There is some degree of public concern over the use of computing environments that are well-known to be publicly-consumable and used for a wide variety of small and large scale uses. There may be a lack of trust as to the effectiveness of the people, technical and process controls that are intended to reduce the risks of confidentiality and breach to manageable levels. One should be comfortable with any challenge that comes from the public and the media. And if there is a security incident, then the question will be raised as to why public cloud was used.

A.2.2.4.3 Lock in and migration

If you build your infrastructure using standard and widely available components such as virtual machines (VMs) and storage, it will ease any migration to another provider. However, vendor specific components are attractive as they may provide lower cost options and facilitate faster delivery. Be conscious of any trade-off. Consider the impact of the necessity of migrating potentially large quantities of data to launch a service, and the potential future impact of increased data scale if ever you wished to, or needed to, migrate to an alternative.

A.2.2.4.4 Data repatriation

Consider how any data within the system can be retrieved and returned to you when the contract for cloud services expires. Discuss with your intended provider how you wish your data to be transferred back into your custody. Ensure such facilities and associated timescales are agreed and included within the contract. You should also seek assurances from your cloud provider that any copies of your data will be deleted, overwritten or otherwise rendered inaccessible.

A.2.2.4.5 Existing situation

When considering moving systems into public cloud, it is worth considering the "As-Is" hosting solution. If you have an existing high risk but low security solution, then the perceived risks of moving into a public cloud might be mitigated.

A.2.2.4.6 Complex systems

Systems can host a variety of different data types, which hold different risk profiles. It might be appropriate to consider hosting some subsystems on public cloud whilst hosting other subsystems elsewhere.

A.2.2.4.7 Data residency and sovereignty

Some cloud providers might store or process data offshore, which might improve resilience and reduce costs. Processing data in cloud services is legally complex, regardless of where the data is being processed. Careful consideration should be given to the country that is used to host data storage to ensure that it is adequate.

A.2.2.4.8 Fair Processing

Regardless of the where services are hosted, organizations processing personal data are typically expected to do so fairly and lawfully. This might be set out in local data protection regulations. Fair processing includes providing details of

— your identity,

— the purpose or purposes for which you intend to process the information, and

— any extra information you need to give individuals in the circumstances to enable you to process the information fairly.

A.2.2.5 Documentation

It is important that a complete set of documentation is kept for audit purposes to prove that appropriate due diligence has been taken with regards to where and how data is hosted. Therefore, document should include the following:

a) The governance decision to use the cloud (e.g. meeting minutes).

b) Responses to all other considerations listed above.

A.2.2.6 Contracts

All Cloud contracts need to be robust and clearly compliant with local law. It is essential to have documentation that details what duties and obligations have been agreed on.

A.2.3 Recommendation 3 – Implement

A.2.3.1 General

Once it is decided to utilise public cloud to host the system, the typical next steps would include the following:

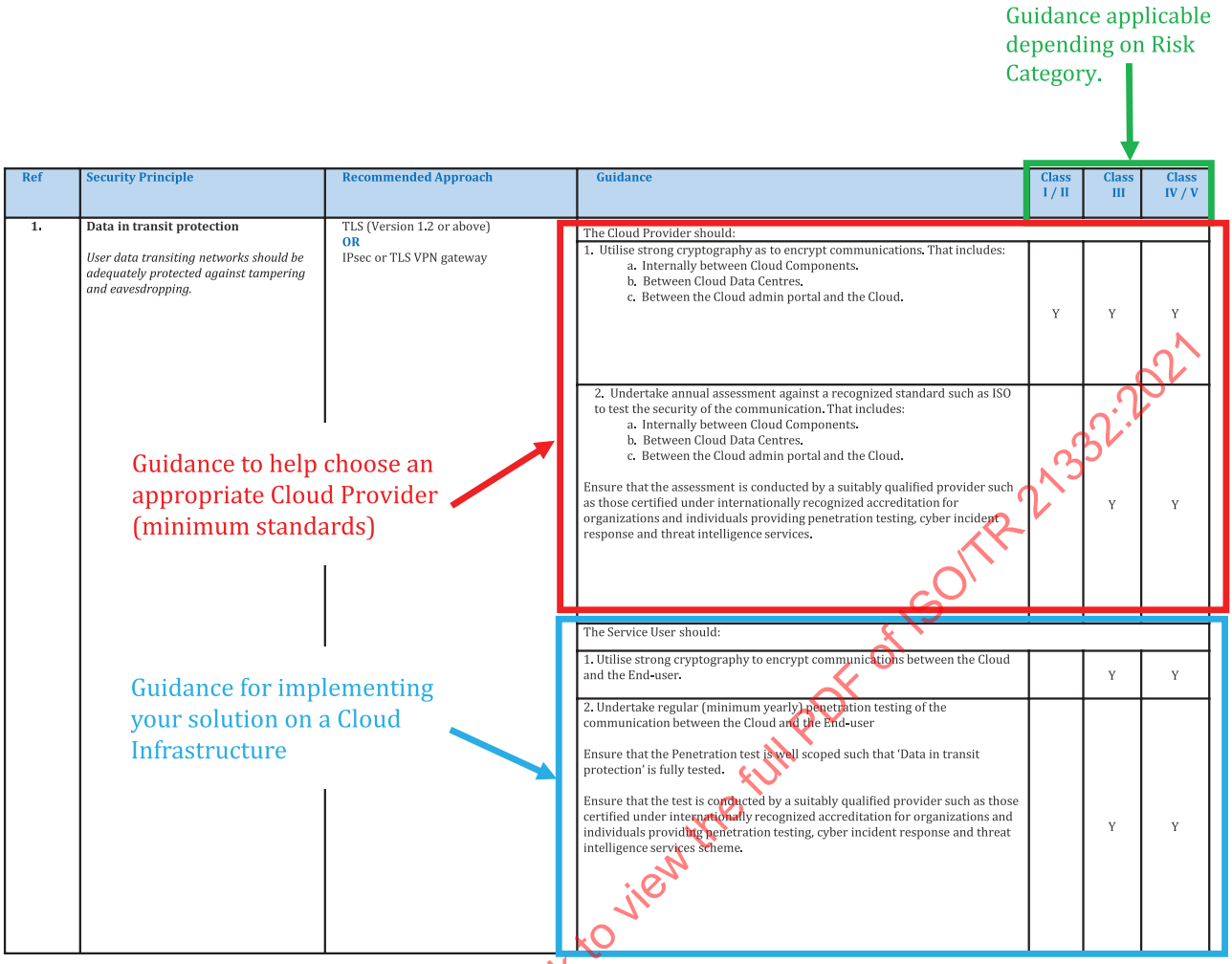
— select a cloud provider that meets the required security standards, and

— apply the security controls that are under your responsibility.

Using public cloud necessitates a joint responsibility to security. The cloud provider ensures that their service is appropriately secure, and to the users should have confidence in it. Similarly, the users have a responsibility to ensure how they implement the solution is appropriately secure. This is often referred to as the joint responsibility model.

Annex B lists the minimum standards the cloud provider can meet and how you should implement the solution. Against each principle is the recommended approach and specific guidance, dependant on the risk classification. The list is presented in Figure A.1.

NOTE Physical resilience and availability uses the service category (B)ronze, S(ilver), G(old) and (P)latinum, rather than Cat I to V, to determine which minimum standards / controls that need to be in place.



Ref	Security Principle	Recommended Approach	Guidance	Class I / II	Class III	Class IV / V
1.	**Data in transit protection** *User data transiting networks should be adequately protected against tampering and eavesdropping.*	TLS (Version 1.2 or above) **OR** IPsec or TLS VPN gateway	The Cloud Provider should:			
			1. Utilise strong cryptography as to encrypt communications. That includes: a. Internally between Cloud Components. b. Between Cloud Data Centres. c. Between the Cloud admin portal and the Cloud.	Y	Y	Y
			2. Undertake annual assessment against a recognized standard such as ISO to test the security of the communication. That includes: a. Internally between Cloud Components. b. Between Cloud Data Centres. c. Between the Cloud admin portal and the Cloud. Ensure that the assessment is conducted by a suitably qualified provider such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.		Y	Y
			The Service User should:			
			1. Utilise strong cryptography to encrypt communications between the Cloud and the End-user.		Y	Y
			2. Undertake regular (minimum yearly) penetration testing of the communication between the Cloud and the End-user Ensure that the Penetration test is well scoped such that 'Data in transit protection' is fully tested. Ensure that the test is conducted by a suitably qualified provider such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services scheme.		Y	Y

Figure A.1 — Example of the use of Table B.1 and its content

A.2.3.2 Select a cloud provider

Choose a cloud provider that meets the minimum-security standards as specified in Table B.1. Each of the 14 principles will have a section entitled "The cloud provider should:" This lists a set of minimum standards. However, you only need to adopt the standard that corresponds to your risk score. For example, if your risk score is Class II, then in the above example, the Cloud provider only needs to meet requirement 1. However, if your risk score is Class IV then they need to meet requirements 1 and 2.

You may need to request further information from the supplier to be confident that they meet the recommended standards.

A.2.3.3 Apply security controls

Similarly, you can implement controls in-line with the recommendations in Table B.1. Each of the 14 principles will have a section entitled "The service user should:" This lists a set of minimum implementation standards. However, you only need to adopt the standard that corresponds to your risk score. For example, if your risk score is Class II, then in the above example you have no controls to apply. However, if your risk score is Class IV then you should meet requirements 1 and 2.

A.2.3.4 Documentation

It is important that a complete set of documentation is kept for audit purposes to prove that appropriate due diligence has been taken with regards to where and how data is hosted. Therefore, document and retain, for example, the following:

a) Evidence that the supplier meets the standard.

b) Evidence that you have implemented the controls.

c) Cloud contract(s), showing that they are clearly compliant with UK law and what duties and obligations have been agreed.

A.2.4 Recommendation 4 – Monitor

A.2.4.1 General

Like any other system, once implemented you cannot forget about security and risk. It needs to be proactively monitored and managed.

A.2.4.2 Manage known risk

If there are any residual risks, then these need to be documented and pro-actively managed.

A.2.4.3 Monitor cloud service

Cloud services offered by providers are most likely to continually evolve. You need to make sure that your vendor keeps you informed of any changes that may affect, in a detrimental way, the security of your system and data.

Similarly, your vendor should supply updated proof of certifications and assessments on a regular basis.

A.2.4.4 Monitor controls

The service user is responsible for implementing and maintaining certain security controls. These should be reviewed/audited on a regular basis.

Annex B
(informative)

Detailed advice and guidance

Table B.1 is based on a jointly published paper by the Department of Health and Social Care, NHS England, NHS Digital[10] and NHS Improvement, Section 8 and states that the NHS and social care organizations can safely locate health and care data, including confidential patient information, in the public cloud including solutions that make use of data off-shoring on its Appendix A on Detailed Advice and Guidance. These principles have been examined within the context of health and social care and a recommended implementation approach has been specified. Further, guidance has also been listed against each principle, detailing what the Cloud Provider should do/provide. It also lists what the Cloud Service User should do to safeguard data.

These recommendations assume that an Infrastructure as a Service (IaaS) model is used and the split of responsibilities between the Cloud Provider and Cloud Service User reflects this. When a SaaS model is utilized then the split would need to be adjusted with the SaaS provider taking more of the responsibilities.

For clarity, the "Cloud Provider" is the organization that is providing the cloud service. The "Service User" refers to the customer-side architect / developer / programmer / IT Pro / etc. that is developing and maintaining the system in the public cloud.

The specific guidance is only applicable if there is a "Y" in the category field that matches the data risk category as defined by the risk tool. Section 2.6 on Physical resilience and availability – is an exception. The "Y" relates to the Service Classification4, being either Bronze, Silver, Gold or Platinum.

Table B.1 — Recommended approach for Implementing the Cloud Security Principles within the context of health and social care

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
1.	**Data in transit protection** *User data transiting networks should be adequately protected against tampering and eavesdropping.*	TLS (Version 1.2 or above) **OR** IPsec or TLS VPN gateway	The Cloud Provider should:			
			1. Utilise strong cryptography as to encrypt communications. That includes: a. Internally between Cloud Components. b. Between Cloud Data Centres. c. Between the Cloud admin portal and the Cloud.	Y	Y	Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
			2. Undertake annual assessment against a recognized SDO such as ISO to test the security of the communication. That includes: a. Internally between Cloud Components. b. Between Cloud Data Centres. c. Between the Cloud admin portal and the Cloud. Ensure that the assessment is conducted by a suitably qualified provider such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.		Y	Y
			The Service User should:			
			1. Utilise strong cryptography to encrypt communications between the Cloud and the End-user.		Y	Y
			2. Undertake regular (minimum yearly) penetration testing of the communication between the Cloud and the End-user Ensure that the Penetration test is well scoped such that 'Data in transit protection' is fully tested. Ensure that the test is conducted by a suitably qualified provider such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services scheme.		Y	Y
2	Asset protection and resilience User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.					

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
2.1	**Physical location and legal jurisdiction** *In order to understand the legal circumstances under which your data could be accessed without your consent you can identify the locations at which it is stored, processed and managed.* *You will also need to understand how data-handling controls within the service are enforced, relative to UK legislation.*	Known locations for storage, processing and management	The Cloud Provider can: 1. Provide cloud infrastructure (which includes all hardware, software, networks and the physical data centres that house it all) to provide companies with a mechanism to comply with data protection requirements when transferring personal data.	Y	Y	Y
			2. Provide independent validation that the data centres are actually physically located to provide companies with a mechanism to comply with data protection requirements when transferring personal data.	Y	Y	Y
			3. State the legal jurisdiction(s) to which your data is subject.	Y	Y	Y
			The Service User should: 1. Only use Cloud Infrastructures to store and process data that are physically located to provide companies with a mechanism to comply with data protection requirements when transferring personal data.	Y	Y	Y
			2. Review the Cloud Provider's Terms and Conditions to ensure they are compliant with the local Data Protection Act and the General Data Protection Regulation.	Y	Y	Y
2.2	**Data centre security** *Locations used to provide cloud services need physical protection against unauthorized access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.*	Conforms to a recognized standard	The Cloud Provider should: -			
			1. Hold and maintain certification to ISO/IEC 27001[2]. Prove that the scope of certification includes the physical security of the data centres. The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.	Y	Y	Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
2.3	**Data at rest protection** *To ensure data is not available to unauthorized parties with physical access to infrastructure, user data held within the service should be protected regardless of the storage media on which it's held.* *Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.*	Encryption of all physical media1.	The Cloud Provider should:			
			1. Provide encryption facilities to ensure that no data is written to storage in an unencrypted form.	Y	Y	Y
			2. Provide secure key management service providing strong cryptography. The service can provide detailed audit reporting on access of the keys	Y	Y	Y
			3. Confirm that the encryption utilises strong cryptography.	Y	Y	Y
			4. Undertake annual assessment against a recognized standard from SDO such as ISO to test the encryption. Ensure that the test is conducted by a suitably qualified provider such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.		Y	Y
			The Service User should: -			
			1. Ensure that the encryption is appropriately configured when you implement the system on your chosen cloud provider.	Y	Y	Y
			2. Ensure keys are managed by the data controller. Keys can be stored either locally or in an HSM service provided by the cloud supplier the key management solution should utilise strong cryptography.	Y	Y	Y
2.4	**Data sanitization** *The process of provisioning migrating and de-, provisioning resources should not result in unauthorized access to user data.*	Explicit overwriting of storage before reallocation	The Cloud Provider should:			
			1. Provide assertions regarding their data sanitization approach.	Y	Y	Y
			2. Show that the specified data sanitation approach has been validated by a suitably qualified independent third party.		Y	Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
2.5	**Equipment disposal** *Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service.*	A recognized standard for equipment disposal is followed **OR**	The Cloud Provider should: -			
			1. Hold certification as recommended by ISO/IEC 27001[2]. Prove that the scope of certification validates the secure equipment disposal. The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.		Y	Y
		A third-party destruction service is used	The Cloud Provider should: -			
			1. Ensure the security of the equipment and prove the chain of custody until the equipment is successfully destroyed.		Y	Y
			2. Demonstrate that the third-party services have been assessed against a recognized standard. Prove that the scope of the assessment validates the secure equipment disposal and chain of custody. Demonstrate that the assessment was performed by a suitably qualified expert party such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.		Y	Y
2.6	**Physical resilience and availability** *Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business*	The service provider commits to a Service Level Agreement (SLA) **AND** Analysis of the design	**Service Classification (See Annex B):**	**B**	**S**	**G/P**
			The Cloud Provider should:			
			1. Provide a contractual commitment to SLAs, with remedies available should the SLA be missed.	Y	Y	Y
			2. Prove that the data centres are certified to Uptime Institute Tier 2 or equivalent qualified provider such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.	Y		

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
			3. Prove that the data centres are certified to Uptime Institute Tier 3 or equivalent qualified provider such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.		Y	Y
			4. Provide two or more "availability zones" / Data Centres in-line with the requirements in 2.1.		Y	Y
			The Service User should:			
			1. Design for failure. Solutions should be architected for cloud such that they are resilient regardless of the underlying cloud infrastructure.	Y	Y	Y
			2. Use at least one availability zone / Data Centre.	Y		
			3. Have resilient network links to the zone / Data Centre.	Y		
			4. Use multiple availability zones / Data Centres.		Y	
			5. Have resilient network links to each zone / Data Centres.		Y	
			6. Use different cloud vendors or multiple regions from the same vendor.			Y
			7. Have resilient network links to each region / vendor.			Y
			8. Ensure their system has DDoS protection. This may be provided by the Cloud vendor or a third party.			
3	**Separation between users** *A malicious or compromised user of the service should not be able to affect the service or data of another.*	Virtualization technologies (e.g. a hypervisor) provide separation between users **OR** Other software provides separation between users	The Cloud Provider should: -			
			1. Provide Supplier Assertions regarding their approach to user/ customer environment separation.	Y	Y	Y
			2. Undertake annual assessment against a recognized standard from SDO such as ISO to test the 'separation between users/ customer environment'. Ensure that the test is conducted by a suitably qualified provider such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.		Y	Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
			3. Hold and maintain certification to ISO/IEC 27017[5] for the Cloud Platform. The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.		Y	Y
			The Service User should: -			
			1. Undertake end-to-end Penetration testing of the solution.		Y	Y
			2. Implement a GPG13 compliant Protective Monitoring solution.			Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
4.	**Governance framework** *The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.*	Conformance with a recognized standard	The Cloud Provider should: -			
			1. Hold and maintain certification as recommended by ISO/IEC 27001[2]. The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.		Y	Y
			2. Prove that the scope of certification includes the governance framework goals set out below: a. A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'. b. A documented framework for security governance, with policies governing key aspects of information security relevant to the service. c. Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk. d. Processes to identify and ensure compliance with applicable legal and regulatory requirements.			Y
5	**Operational security** *The service needs to be operated and managed securely in order to impede detect or prevent attacks., Good operational security should not require complex bureaucratic, time, consuming or expensive processes.*					

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
5.1	**Configuration and change management** *You should ensure that changes to the system have been properly tested and authorized. Changes should not unexpectedly alter security properties*	Conformance with a recognized standard	The Cloud Provider should:			
			1. Hold and maintain certification as recommended by ISO/IEC 27001[2]. Prove that the scope of certification includes configuration and change management processes. The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.			Y
			The Service User should: -			
			1. Maintain an accurate inventory of the assets which make up the service, along with their configurations and dependencies.	Y	Y	Y
			2. Ensure changes to the service are assessed for potential security impact, and the implementation of changes are managed and tracked through to completion.	Y	Y	Y
5.2	**Vulnerability management** *You should identify and mitigate security issues in constituent components*	Conformance with a recognized standard	The Cloud Provider should:			
			1. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001,[2] ISO/IEC 27017[5]. The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.	Y	Y	Y
			2. Manage vulnerabilities in a manner that aligns with ISO/IEC 30111 and show ISO / CSA compliance to validate the process.	Y	Y	Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
			3. Prove that mitigations for discovered vulnerabilities are implemented for the server-less devices, hypervisors and supporting infrastructure, within the NCSC best practice timescales set out below: a. 'Critical' vulnerabilities should be mitigated within 24 hours b. 'Important' vulnerabilities should be mitigated within 2 weeks. c. 'Other' vulnerabilities mitigated within 8 weeks. If compensating controls are in place to reduce the vulnerability risk, the timescales can be adjusted accordingly.	Y	Y	Y
			The Service User should: -			
			1. Undertake patching or vulnerability management for the guest operating system and application components, within the best practice timescales set out below: a. 'Critical' patches should be deployed within 24 hours b. 'Important' patches should be deployed within 2 weeks of a patch becoming available c. 'Other' patches deployed within 8 weeks of a patch becoming available		Y	Y
			Undertake regular (min yearly) penetration testing. Ensure that the Penetration test is well scoped such that 'security vulnerabilities in the Operating system and components above' are fully tested. Ensure that the test is conducted by a suitably qualified provider such as those certified under internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.		Y	Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
5.3	**Protective monitoring** *You should put measures in place to detect attacks and unauthorized activity on the service*	Conformance with a recognized standard	The Cloud Provider should:			
			1. Hold and maintain certification as recommended by ISO/IEC 27001[2] and ISO/IEC 27017[5] Prove that the scope of certification includes protective monitoring controls showing that: a. The service generates adequate audit events to support effective identification of suspicious activity b. These events are promptly analyzed to identify potential compromises or inappropriate use of your service c. The service provider takes prompt and appropriate action to address incidents The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.		Y	Y
			The Service User should: -			
			1. Put in place appropriate monitoring solutions to identify attacks against their applications or software.	Y	Y	Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
5.4	Incident management *Ensure you can respond to incidents and recover a secure, available service*		The Cloud Provider should: 1. Hold and maintain certification as recommended by ISO/IEC 27001[2]. Prove that the scope of certification includes incident management controls in detail showing that: a. Incident management processes are in place for the service and are actively deployed in response to security incidents b. Pre-defined processes are in place for responding to common types of incident and attack c. A defined process and contact route exist for reporting of security incidents by consumers and external entities d. Security incidents of relevance to the Service User will be reported in acceptable timescales and formats The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.	Y	Y	Y
			2. Demonstrate robust, well tested and rehearsed incident management procedures	Y	Y	Y
			The Service User should:			
			1. Put in place monitoring solutions to identify attacks against their applications or software.		Y	Y
			2. Have an incident management process to rapidly respond to attacks		Y	Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
6.	**Personnel security** *Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduce the likelihood of accidental or malicious compromise by service provider personnel.*	Personnel screening performed but does not conforms with BS 7858:2019	The Cloud Provider should: -			
			1. Operate a personnel screening process that aligns with security screening of individuals employed in a security environment and show ISO / CSA compliance to validate the process. Demonstrate that the assessment was performed by a suitably qualified expert party such internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services.		Y	Y
			The Service User should: -			
			1. Ensure IT admin staff are strongly authenticated.		Y	Y
			2. Have a suitable auditing solution is in place to record all IT admin access to data and hosting environments.		Y	Y
7.	**Secure development** *Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.*	Independent review of engineering approach against recognized secure development standard	The Cloud Provider should: -			
			1. Hold and maintain certification to: a. ISO/IEC 27034, or b. ISO/IEC 27001 [2] The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.		Y	Y
8.	**Supply chain security** *The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.*	Assessed through application of appropriate standard	The Cloud Provider should:			
			1. Hold and maintain certification to: a. ISO/IEC 27001 [2], or b. ISO 28000:2007 The certification should be conducted by a certification body meeting the requirements of ISO/IEC 27006.		Y	Y

Table B.1 *(continued)*

Ref	Security Principle	Recommended Approach	Guidance	Class I / IIs	Class III	Class IV / V
			2. Prove that the scope of certification includes supply chain security showing: a. How your information is shared with, or accessible to, third party suppliers and their supply chains. b. How the service provider's procurement processes place security requirements on third party suppliers. c. How the service provider manages security risks from third party suppliers. d. How the service provider manages the conformance of their suppliers with security requirements. e. How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.			Y
9	**Secure user management** *Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorized access and alteration of your resources, applications and data.*					
9.1	**Authentication of [admin] users to management interfaces and support channels** *In order to maintain a secure service, [admin] users need to be properly authenticated before being allowed to perform management activities, report faults or request changes to the service.*	Strong authentication in place, which is subject to regular exercising	The Cloud Provider should: -			
			1. Provide Supplier Assertions regarding their approach to strong authentication	'Y	Y	Y
			2. List all the channels by which the service provider would accept. management or support requests from you (telephone phone, web portal, email etc.).	Y	Y	Y