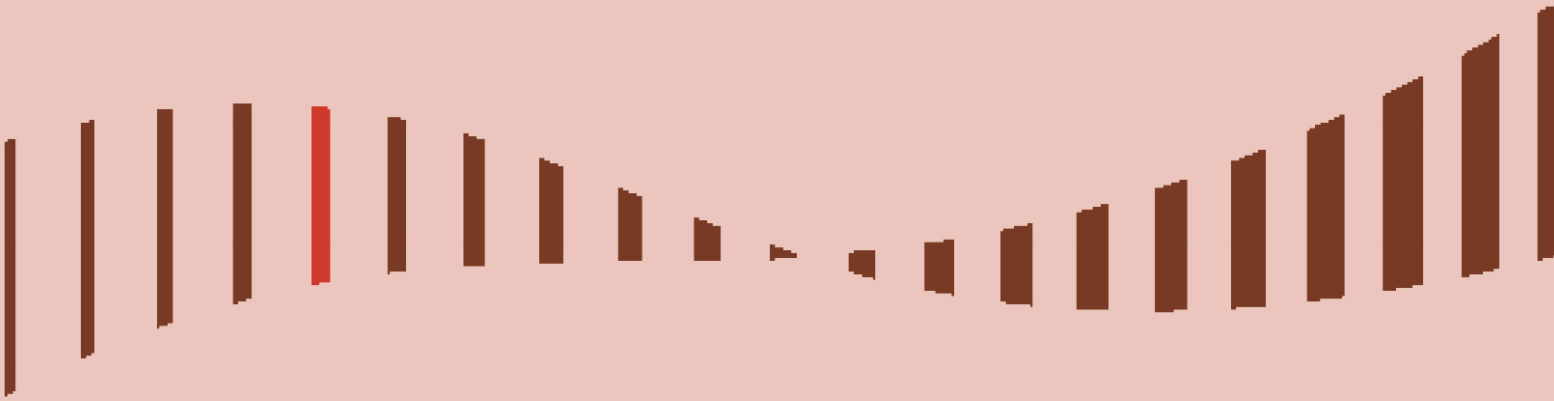
V 1.1

HDH CERTIFICATION REFERENCE SYSTEM

Requirements and controls

Version 1.1 - June 2018



This document is the English version of HDH certification reference system – requirements and controls v1.1. In case of litigation, only the French version shall be considered as authentic, valid and taken into consideration for any purpose of interpretation.

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Reference documents

Reference no. 1: NF ISO/IEC 27001:2013
Information technology – Security techniques – Information security management systems -- Requirements

Reference no. 2: ISO/IEC 27018:2014
Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Reference no. 3: NF ISO/IEC 20000-1:2011
Information technology – Service management – Part 1: Service management system requirements

Reference no. 4: HDH accreditation reference system

Contents

1.Introduction

1.1. Purpose of this document

This document constitutes the certification reference system applicable to hosts wishing to obtain certification for the scope of “physical infrastructure provider” or “IT managed services provider”[1] of personal health data.

Hereinafter, this health data hosting reference system is referred to by the term HDH reference system.

1.2. Structure of the document

This document is divided into four sections:

1. introduction;

2. presentation of the international standards adopted within the context of personal health data hosting certification;

3. list of acronyms used in the HDH certification reference system;

4. list of the requirements of the HDH reference system relating to the two scopes of certification as “physical infrastructure provider” or “IT managed services provider”.

[1] The “physical infrastructure provider” and “IT managed services provider” scopes are described in the document
Reference no. 4: HDH accreditation reference system.

2.Normative references

The standards referenced in this document are listed below.

NF ISO/IEC 27001: December 2013, *Information technology – Security techniques – Information security management systems - Requirements*

NF ISO/IEC 20000-1: June 2012, *Information technology – Service management - Part 1: Service management system requirements*

ISO/IEC 27018:2014, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

For ease of reading, the above standards will be referred to herein as follows:

- NF ISO 27001 for standard NF ISO/IEC 27001: December 2013;
- NF ISO 20000-1 for standard NF ISO/IEC 20000-1: June 2012;
- ISO 27018 for standard ISO/IEC 27018:2014.

3.Acronyms used

:

SoA	Documented Statement of Applicability describing the security objectives, and the appropriate measures applicable to an organization's ISMS
HDH	Health Data Host or Health Data Hosting
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
CB	Certification Body
ISMS	Information Security Management System

4. Requirements of the HDH certification reference system

This chapter sets out the requirements of the HDH reference system.

4.1. Links between requirements and standards

The HDH reference system requirements defined hereafter are derived, on the one hand, from existing standards and, on the other hand, from requirements defined specifically for HDH certification.

The HDH reference system thus includes:

- the requirements under standard NF ISO 27001 taken as a whole;
- part of the requirements listed in standard NF ISO 20000-1;
- additional requirements under standards NF ISO 27001 and NF ISO 20000-1;
- requirements relating to the protection of personal health data, identified as main requirements in chapter 4, for which compliance with the requirements of standard ISO 27018 may give rise to a presumption of conformity;
- requirements relating to the protection of personal health data, identified as additional requirements in chapter 4;
- requirements specific to the healthcare sector.

4.2. Requirements under NF ISO 27001

Physical infrastructure providers and IT managed services providers must be certified to NF ISO 27001.

In addition, the following specific requirements supplementing NF ISO 27001 apply.

Additional requirement (chapter 4.3 of standard NF ISO 27001)

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must determine the scope of the information security management system (ISMS) taking into account the objective to protect personal health data in addition to the issues and requirements already considered.

This scope of application must at least cover all of the provider's personal health data hosting activities.

Additional requirement (chapter 6.1.3 of standard NF ISO 27001)

Application: Physical infrastructure providers and IT managed services providers.

Objective: The SoA (Statement of Applicability) of the ISMS must include all the requirements of the HDH certification reference system.

Any exclusion of the requirements of the scope of certification must be formally justified and the justification must be approved by the certification body.

Additional requirement (Annex A12.3 of standard NF ISO 27001)

Application: IT managed services providers

Objective: In the event of the outsourcing of health data backups, the host must guarantee the security of such backups, whatever the backup medium.

Implementation recommendations:

- The ISMS takes into account the health data backups, in particular their security according to criteria relating to confidentiality, integrity and traceability during transfers and throughout the retention of the data;
- Backup security measures are implemented.

Additional requirement (Annex A12.7 of standard NF ISO 27001)

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must allow its customers to perform audits on the applications brought into service.

Method of control:

- Ensure that the IT managed services provider has defined, documented and implemented a procedure governing the performance of audits by its customers, in particular security audits (penetration tests, etc.);
- The items for which the provider is responsible, in particular shared items, may be excluded from the customers' scope of audit; in such a case, it is necessary to ensure that the provider is able to provide its customers with the results of an independent external audit of such items.

4.3. Requirements under NF ISO 20000-1

Within the context of HDH certification, only the following requirements of standard NF ISO 20000-1 apply.

4.3.1. Planning of new or changed services

Chapter 5.2 of standard NF ISO 20000-1 applies to physical infrastructure providers and IT managed services providers.

4.3.2. Design and implementation of new or changed services

4.3.2.1. Presentation of activities performed by service providers, customers and other parties

Chapter 5.3 (b) of standard NF ISO 20000-1 applies to physical infrastructure providers and IT managed services providers.

In addition, the following specific requirement supplementing standard NF ISO 20000-1 applies.

Additional requirement (chapter 5.3 of standard NF ISO 20000-1)

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must define acceptance criteria for any new service or for any change to a service and must perform acceptance tests before they are brought into service.

Method of control:

- Ensure that the IT managed services provider has set up a methodology for the verification of the applications that it hosts;
- Verify that the IT managed services provider has formalized a procedure to define hosting prerequisites and a procedure to verify these prerequisites (the prerequisites must include, at the very least, the installation instructions and the operating instructions);
- Verify that the IT managed services provider has formalized a structured test and validation process providing objective proof that the future service will not disrupt the overall performance of the hosted system and will not impair its level of security.

4.3.3. Service continuity and availability management

4.3.3.1. Service continuity and availability management requirements

Chapter 6.3 of standard NF ISO 20000-1 applies to physical infrastructure providers and IT managed services providers.

4.3.3.2. Capacity management

Chapter 6.5 of standard NF ISO 20000-1 applies to physical infrastructure providers and IT managed services providers.

4.4. Requirements relating to the protection of personal health data

The requirements relating to the protection of personal health data listed hereafter apply. A provider who has implemented the provisions and measures specified in standard ISO 27018 will be presumed to conform to the so-called main requirements. This presumption of conformity does not cover the so-called additional requirements.

4.4.1. Rights of the data subjects

4.4.1.1. Obligation to cooperate

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must make available the procedures and means to enable its customers to respond to requests from data subjects to exercise their rights. The rights covered are those defined in articles 15 to 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

4.4.2. Purpose

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must process personal data only on documented instructions from its customer and must not depart from the purposes stated in the instructions. These instructions must be documented within the framework of the agreement entered into with the customer.

Additional requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must not use the health data that it hosts for any purposes other than the performance of the hosting services. In particular, it is prohibited from using said data for marketing, advertising, commercial or statistical purposes.

4.4.3. Disclosure of data

4.4.3.1. Temporary data

Main requirement

Application: IT managed services providers.

Objective: The provider must define a data retention period and comply with this deadline. The provider must document and set up the means to ensure that temporary data is deleted upon the expiry of this deadline.

4.4.3.2. PII disclosure notification

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: Court-ordered seizures that include personal data must be governed contractually. A procedure must define the conditions under which such a transfer is notified to the customer, unless such notification is prohibited.

4.4.3.3. Recording of PII disclosures

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must keep a log of the transmission of personal data to third parties containing the following information at minimum: a list of the data transmitted, the recipient(s) and the dates of disclosure.

4.4.3.1. Integrity and acknowledgement of exchanges

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: Personal data transmitted via a communication network must be subject to controls to ensure that the data has indeed been received by the target system.

4.4.4. Transparency

4.4.4.1. Disclosure of subcontracted PII processing

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provisions of the agreements entered into between the provider and its customer must specify any recourse to the subcontracting of personal data processing. Thus, the provider must not use a subcontractor without having first informed the customer.

4.4.5. Accountability

4.4.5.1. Notification of a data breach involving PII

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must notify its customer of any breach of personal data as soon as possible after becoming aware thereof.

4.4.5.2. Retention period for administrative security policies

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The retention periods for the different versions of the security documents must be defined and formalized.

4.4.5.3. PII return, transfer and disposal

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must have defined and formalized a policy governing the making available and return of personal data to the provider's customers, as well as the destruction of the data. This policy must be provided to customers upon request.

Additional requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: A reversibility procedure defining the methods of return of the data at the end of the contract or upon withdrawal of certification must be formalized and applied.

4.4.6. Information security

4.4.6.1. Confidentiality or non-disclosure agreements

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The employment contracts of the provider's employees must include a confidentiality clause. In the event of recourse to subcontracting, this requirement also applies to the subcontractors.

4.4.6.2. Restriction on the use of paper copies

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must restrict the use of paper copies.

4.4.6.3. Control and logging of data restoration

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must have a procedure governing data restoration. Any restoration operations performed must be logged.

4.4.6.4. Protecting data on storage media leaving the premises

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: Prior authorization must be obtained for portable storage media containing personal data to leave the provider's premises. Such data must be made inaccessible to unauthorized personnel, for example by protecting it using state-of-the-art encryption.

4.4.6.5. Use of portable storage media and devices

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The use of portable storage media and devices that are incompatible with encryption solutions must be prohibited.

4.4.6.6. Encryption of personally identifiable data transmitted over public data-transmission networks

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: Personal data must be encrypted before being transmitted over public networks.

4.4.6.7. Secure disposal of paper copies

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: Paper copies must be destroyed using appropriate means.

4.4.6.8. Unique use of user IDs

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: Access to personal data or to systems used to process personal data must be through nominative accounts.

Additional requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: Means of traceability must be implemented in order to control the actions and utilization of generic IDs.

Method of control:

The certification body must:

- Ensure that the generic ID management policy limits their use to identified specific cases, for example due to constraints inherent to certain hardware or software;
- Ensure that nominative, time-stamped logs of the use of generic IDs are included in the logging and monitoring policy.

4.4.6.9. Records of authorized users

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: A process to manage user authorizations must be defined and applied. In particular, an up-to-date record should be maintained of the users or profiles of users who have access to personal data or to the information systems used to process personal data.

4.4.6.10. Logging and monitoring

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must implement the means to ensure the logging and monitoring of user activities, faults and events related to information security. Event logs must be kept and regularly reviewed. The provider must ensure the integrity of the event logs and protect them against unauthorized access.

In addition, system administrator and system operator activities must be logged and the logs protected and regularly reviewed.

In order to guarantee the reliability of the logs, the provider must synchronize the clocks of all the systems (to a single reference time source).

Additional requirement

Application: IT managed services providers.

Objective: Technical and organizational means must be implemented in order to communicate administrator activity logs to the customer.

Method of control:

- Ensure that the provider has formalized and implemented organizational and technical means in order to process its customers' requests concerning logs of access by the provider's administrators to the hosted health information systems.

4.4.6.11. User ID management

Main requirement

Application: IT managed services providers.

Objective: De-activated or expired user IDs should not be assigned to other individuals.

4.4.6.12. Contract measures

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: Contracts between the provider and its customers must specify the technical and organizational measures provided for to meet the objectives for the security and protection of personal data, as well as the processing purposes. Changes in these measures must not result in the level of security being reduced without the prior agreement of the customer.

4.4.6.13. Subcontracted personally identifiable data processing

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: In the event of the provider having recourse to subcontracting, the related contract must specify the technical and organizational measures provided for to meet the objectives for the security and protection of personal data. Changes in these measures must not result in the level of security being reduced without the prior agreement of the provider. The provider must ensure that this level of security is in line with its commitments to its customers.

4.4.6.14. Access to data on pre-used data storage space

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must ensure that in the event of the re-use of storage space, the latter has first been purged and that no old data can be accessed.

4.4.7. Location of data

4.4.7.1. Geographical location of personally identifiable data

Main requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must list all the countries in which the customer's data is or might be stored.

Additional requirement

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must inform the customer of the storage locations and allow the latter to choose the country or countries where the health data will be stored and must implement measures to respect this choice.

4.5. Additional requirements

4.5.1. Roles and responsibilities

Application: Physical infrastructure providers and IT managed services providers.

Objective: The division of responsibilities in terms of information security between the provider and its client must be defined and formalized.

4.5.2. Compliance with the enforceable reference systems of the PGSSI-S (Global Information Security Policy for the healthcare sector)

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must inform its customers that they are required to comply with the PGSSI-S (global information security policy for the healthcare sector) and must implement a means of obtaining their commitment to comply with this policy.

Method of control:

- The provider must inform its customers that they are required to implement a health information system in compliance with the PGSSI-S.
- The provider must define and implement a means of obtaining its customers' commitment to comply with the enforceable reference systems of the PGSSI-S. This commitment could be subject to provisions set out in the hosting agreement.

4.5.3. Audit reports

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must provide certification audit reports to any customers who request them. The provider must also provide such reports to the certification body, in the event of transfer or request for recognition of equivalency.

4.5.4. List of customer contacts

Application: Physical infrastructure providers and IT managed services providers.

Objective: The provider must keep a list of points of contact for each customer.

These points of contact must be able to provide the provider with the name of a health professional whenever necessary (examples: access to health data, management of relations with the patient, etc.)

The provider must be able to provide this list immediately to the competent authority upon

request, notably in the event of suspension or withdrawal of certification.

Method of control:

- Verify that the provider's list of customer contacts contains at least the following information:
  - The customer's corporate name;
  - The contact's first and last names;
  - The contact's email address;
  - The contact's telephone number.
- Verify that this list is updated regularly.

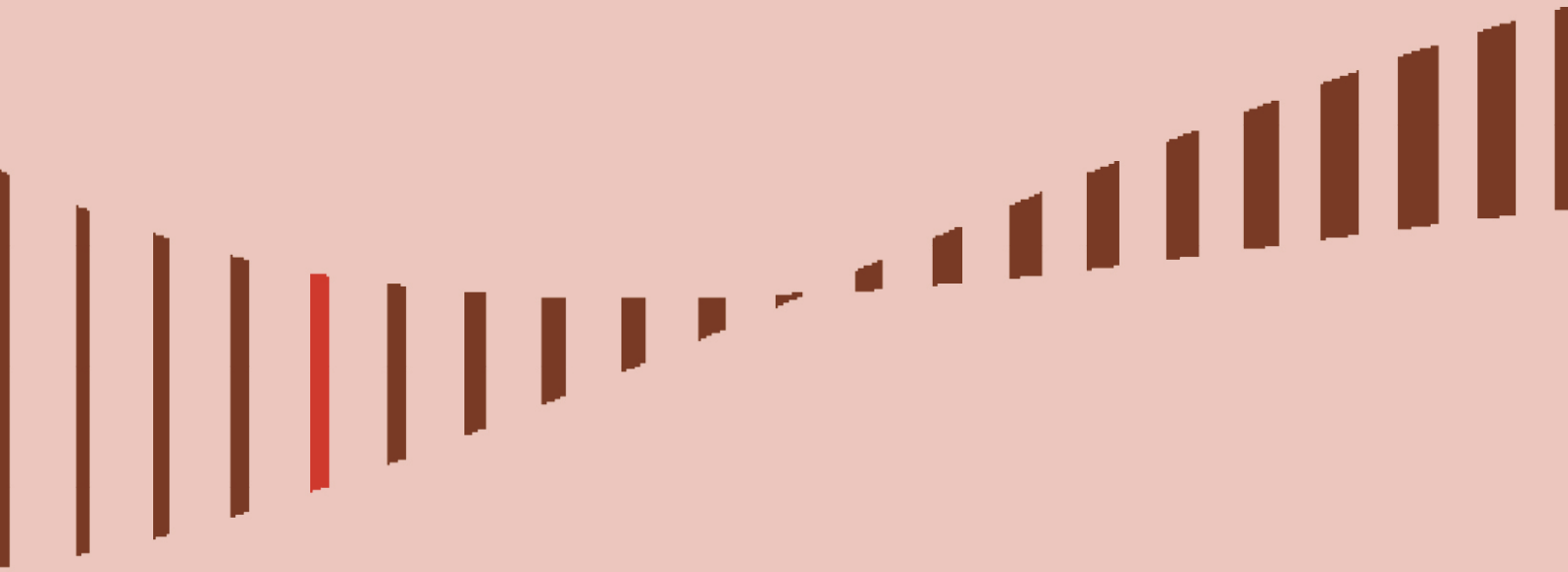
4.5.5. Localization

Application: Physical infrastructure providers and IT managed services providers.

Objective: localization of customer relations.

Method of control:

- Ensure that the user interfaces offered to the customers are available at least in French.
- The provider must provide first-level support at least in French.
- Verify that the SoA is available at least in French.



Agence des Systèmes d'Information Partagés de Santé
9, rue Georges Pitard
Standard : 01 58 45 32 50
Du lundi au vendredi (hors jours fériés)
de 8h30 à 13h et de 14h à 17h
esante.gouv.fr

Requirements and controls