THE FRENCH REPUBLIC

Ministry for Health and Prevention

Order of XXX amending the Order of 11 June 2018 approving the accreditation framework of certification bodies and the certification framework for hosting personal health data

NOR: SPRD2325104A

The Minister of Health and Prevention and the Minister of Economy and Finance,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

Having regard to Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, and in particular notification No XX dated XX;

Having regard to the Public Health Code, with particular reference to Articles L. 1111-8 and R. 1111-10 thereof;

Having regard to Law No 78-17 of 6 January 1978 on data processing, data files and individual liberties, as amended;

Having regard to the Order of 11 June 2018 approving the accreditation framework of certification bodies and the certification framework for hosting personal health data;

Having regard to the opinion of the National Commission on Information Technology and Liberties dated 13 July 2023,

Having regard to notification No…/…/F sent on …. to the European Commission,

Hereby order:

Article 1

Articles 1 and 2 of the above-mentioned Order of 11 June 2018 are replaced by articles worded as follows:

“ *Article 1* - The accreditation framework of certification bodies for hosting personal health data referred to in Article R. 1111-10 of the Public Health Code as amended, annexed to this Order is approved.

" *Art. 2.* - The certification framework for hosting personal health data referred to in Article R. 1111-10 of the Public Health Code as amended, annexed to this Order is approved."

Article 2

The provisions of Article 2 of the Order of 11 June 2018 referred to above, in their wording resulting from this Order, shall enter into force within 6 months of its publication. They shall apply to applications for a certificate of conformity and to applications for the renewal of such a certificate submitted to a certification body from that date.

Article 3

The Minister of Health and Prevention and the Minister of Economy shall each be responsible for the implementation of this Order, which shall be published in the *Official Journal* of the French Republic.

Drawn up on XXX.

For and on behalf of the Minister of Health and Prevention:

Hela Ghariani

Delegate for digital health

For and on behalf of the Minister of Economy and Finance:

Thomas Courbe

Director-General of Companies

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

La transformation commence ici The transformation begins here

Health Data Host (HDS) certification framework

Requirements

Status: Ongoing | *Classification: Restricted* | *Version: v0.1*

Agence du Numérique en Santé (Digital Health Agency)
2 - 10 Rue d'Oradour-sur-Glane – 75015 Paris
Tel. 01 58 45 32 50
esante.gouv.fr

Reference documents

Regulations

Reference	Document
[ART_L1111-8]	Articles L. 1111-8 of the Public Health Code relating to the hosting of health data https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549
[GDPR]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("General Data Protection Regulation") https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
[ART R1111-8-8]	Article R. 1111-8-8 of the Public Health Code relating to the activity of hosting health data https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036656709
[ART R1111-9] to [ART R1111-11]	Articles R1111-9 to R-1111-11 of the Public Health Code relating to the hosting of personal health data on digital media subject to certification. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000006196138/#LEGISCTA000036658495

For further reading

Reference	Document
[ISO 27001]	NF ISO/IEC 27001:2023 Information security, cybersecurity and privacy – Information security management systems – Requirements

Revision History

Version	Date	Comments
V1.1	June 2018	Published version of the Order of 11 June 2018 approving the accreditation framework of certification bodies and the certification framework for hosting personal health data
V1.1.20230330	March 2023	Draft revision, the main modifications of which are: ► The definition of the scope of Activity 5 "Administration and operation of the information system containing health data. ► Taking into account the version of standard NF ISO/IEC 27001: 2023. ► A reminder of the contractual requirements referred to in Article R.1111-11 of the Public Health Code. ► Standardisation of the presentation of guarantees. ► More stringent requirements for data transfers outside the European Union.

CONTENTS

1. PREAMBLE

This update of the certification framework for Health Data Hosts aims to take into account new issues and points for improvement from the previous framework dating from 2018, identified in consultation with the ecosystem. This update consists, particularly, in:

- Improving the readability of the guarantees provided by a Certified Host on the services it performs for a given client;
- Clarifying the contractual obligations of the Host as defined in the Public Health Code;
- More stringent requirements for the protection of personal data in relation to data transfers outside the European Union. On this last point, this is a first step: more stringent requirements in terms of European sovereignty will be added by 2027, consistent with future European frameworks (EUCS – European Cybersecurity Certification Scheme for Cloud Services).

In the event that the Host applying for HDS certification has already obtained certification on the basis of the ANSSI SecNumCloud 3.2 framework, a matrix showing the correspondence between the measures in Annex A of ISO 27001 standard and the SecNumCloud requirements shall be made available to the Hosts in Annex 1 to this framework in order to facilitate the application of a qualified SecNumCloud Host for HDS certification.

1.1. Purpose of the framework

Pursuant to Article R1111-10 of the Public Health Code, the HDS certification framework (hereinafter referred to as “requirements framework” or “framework”) defines the requirements that a Host must meet in order to obtain certification as a Health Data Host.

1.2. Scope of the framework

The requirements framework applies to the Hosts of personal health data referred to in Article L. 1111-8 of the Public Health Code.

2. GENERAL DEFINTIONS AND CONCEPTS

2.1.1. Actor

Any stakeholder contributing to the security of personal health data, excluding the data controller and processors of a certified Host when they act in accordance with the security policy and under the supervision of the said Host.

2.1.2. Administration and operation of the information system containing health data

The activity of administration and operation of the information system containing health data consists in mastering the interventions on the resources made available to the client of the Host. It shall include all of the following ancillary activities:

The definition of a process for the allocation and annual review of nominative, justified and necessary access rights;
Securing the access procedure;
The collection and preservation of traces of the accesses made and the reasons thereof;
Prior validation of interventions (intervention plan, intervention process).

The validation of interventions shall consist in ensuring that they do not degrade the security of the hosted information either for the client concerned or for the other clients of the Host. This validation may be carried out in the following cases:

A priori, for interventions that the client could carry out independently;
When requesting service from the Host.

The definition of the allocation process, security, collection and validation are intrinsic and compulsory to the activities defined in 1 to 4 of Article R. 1111-9 of the Public Health Code. If they are carried out solely insofar as they are related and consubstantial to activities 1 to 4, the Host is not required to be certified for Activity 5. It shall only be required to be so in the event that it only carries out Activity 5.

2.1.3. Client of the Host

The client of the Host (also referred to as “client”) designates the natural or legal person who subscribes to the service provided by the Host.

2.1.4. Host

The Host, also referred to as the organisation in the ISO 27001 standard, is the applicant for certification as Host of health data or for renewal of its certification. It provides all or part of a hosting service for personal health data (or “health data”) within the meaning of Article L. 1111-8 of the Public Health Code.

2.1.5. Electronic identification means

An electronic identification means is a tangible or intangible element containing personal identification data and used to authenticate to an online service.

2.1.6. Data controller

This concept refers to the data controller within the meaning of Regulation 2016/679, i.e. the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing.

2.2. Abbreviations and acronyms

Acronym	
CSP	Code de la santé publique (Public health code)
DSCP	Données de Santé à Caractère Personnel (Personal health data)
HDS	Hébergeur de Données de Santé (Health Data Host)
GDPR	General Data Protection Regulation
ISMS	Information Security Management System

3. SCOPE

3.1. Applicability of the HDS certification framework

The scope of the framework shall be defined by Articles L. 1111-8, R. 1111-8-8 and R. 1111-9 of the Public Health Code.

3.1.1. Role of Host

HDS certification shall apply to any natural or legal person who provides all or part of a hosting service for personal health data and who is a processor within the meaning of Article 28 of the GDPR.

3.1.2. Nature of the data

The hosted data must be personal data relating to health, as defined in Article 4.15 of the GDPR.

3.1.3. Context of the collection

The HDS certification concerns personal health data collected during prevention, diagnosis, care or social or medico-social follow-up activities.

This personal health data must be hosted on behalf of the natural or legal persons responsible for producing or collecting the data or on behalf of the patient.

3.1.4. Activities carried out

Article R. 1111-9 of the CSP shall define the activity of hosting health data:

The provision of all or some of the following activities on behalf of the data controller as mentioned in I(1) of Article R. 1111-8-8 or of the patient as mentioned in I(2) of the same Article shall be considered to be hosting personal health data in

digital format as defined in Article L. 1111-8(II):

1. The provision and maintenance in operational condition of physical sites for hosting the hardware infrastructure of the information system used to process the health data;

2. The provision and maintenance in operational condition of the hardware infrastructure of the information system used to process the health data;

3. The provision and maintenance in operational condition of the virtual infrastructure of the information system used to process the health data;

4. The provision and maintenance in operational condition of the platform for hosting information system applications;

5. The management and operation of the information system containing the health data;

6. Backing up health data.

Activity 5 is specified in paragraph 2.1.2.

Data backup Activity 6 should be interpreted as including only outsourced backups. The backups inherently necessary for Activities 1 to 5 are within the scope of Activities 1 to 5.

4. CONDITIONS FOR AWARDING A CERTIFICATE

Requirement No 01

[REQ 01] The certification of a Host requires:

That it has implemented an Information Security Management System (ISMS) certified in accordance with the ISO 27001 standard, supplemented by the requirements defined in Chapter 5.;
Whereas the scope of this ISMS covers all the Host's health data hosting activities;
Contracts concluded with its clients meet the requirements set out in Chapter 6.;
That it complies with the sovereignty requirements defined in Chapter 7;
That it communicates to its clients the presentation of the guarantees formalised in accordance with the Chapter.

5. ISMS REQUIREMENTS

The numbering of this chapter is aligned with that of ISO 27001 and starts at point 5.4, corresponding to Chapter 4 of the standard.

5.1. Context of the organisation

5.1.1. Understanding the organisation and its context

The requirements set out in Chapter 4.1 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 02
[REQ 02] In determining its external and internal issues, the Host must take into account the fact that its mission requires it to protect the DSCPs entrusted to it by its clients

5.1.2. Understanding the needs and expectations of parties concerned

The requirements set out in Chapter 4.2 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 03
[REQ 03] In determining the requirements of parties concerned, the Host must take into account the applicable legal framework for the protection of DSCP.

5.1.3. Determination of the ISMS scope

The requirements set out in Chapter 4.3 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 04
[REQ 04] The scope of the ISMS must include all DSCP processing provided by the Host. It must cover all the means and processes of processing DSCPs, including backups and transfers of material information media.

5.1.4. Information security management system

The requirements set out in paragraph 4.4 of ISO 27001 shall apply.

5.2. Governance

The requirements set out in Chapter 5 of ISO 27001 shall apply.

5.3. Planning

5.3.1. Actions to be implemented in the face of risks and opportunities

5.3.1.1. General points

The requirements set out in Chapter 6.1.1 of ISO 27001 shall apply.

5.3.1.2. Risk assessment

The requirements set out in Chapter 6.1.2 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 05

[REQ 05] When assessing risks, the Host must at least consider the following events:

A. Failure of material information media due to physical and environmental threats.
B. Loss of control of material information media, in particular during:
    a. Copying DSCPs on portable media;
    b. Any materialisation in paper format;
    c. Reallocation of storage spaces.
C. Damage, compromise or interruption of an internal or external information flow under the responsibility of the Host.
D. Failure to control the access granted, whether to staff under the control of the organisation or to those designated by its clients:
    a. Allocation, modification and withdrawal of access rights;
    b. Distribution of electronic identification means;
    c. Traceability and accountability of access;
    d. Occasional access during audits and intrusion tests.
E. Failure to control interventions, whether at the initiative of the organisation or commissioned by a client.
F. Unforeseen use of the service due to clumsiness or malicious intent.
G. Hardware or software failures, with inability to meet business continuity or recovery commitments.
H. Subjection of the Host or any processors to non-European legislation which may result in a breach of the DSCP.

5.3.1.3. Risk treatment

The requirements set out in Chapter 6.1.3 of ISO 27001 shall apply taking into account the following requirements.

Requirement No 06

[REQ 06] Where subcontracting is used, the Host must ensure that it controls changes to the technical and organisational measures of its processors to deal with the identified risks.

Requirement No 07

[REQ 07] In order to reduce the risk of unforeseen use of the system, the Host must ensure that:

The interfaces offered to clients are available at least in French;
The first level support is at least in French.

Requirement No 08

[REQ 08] The declaration of applicability must be available in French to auditors on request.

5.3.2. Information security objectives and plans to achieve them

The requirements set out in Chapter 6.2 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 09

[REQ 09] The information security objectives established by the Host must include the protection of DSCPs entrusted to it by its clients and include compliance with the obligations of the GDPR.

5.3.3. Planning of changes

The requirements set out in Chapter 6.3 of ISO 27001 shall apply.

5.4. Media

5.4.1. Resources

The requirements set out in paragraph 7.1 of ISO 27001 shall apply.

5.4.2. Competence

The requirements set out in paragraph 7.2 of ISO 27001 shall apply.

5.4.3. Awareness

The requirements set out in Chapter 7.3 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 10

[REQ 10] Staff working for the Host must be made aware of the criticality in terms of availability, confidentiality and integrity of hosted DSCPs.

This requirement also applies to the staff of any processors of the Host.

5.4.4. Communication

The requirements set out in Chapter 7.4 of ISO 27001 shall apply taking into account the following requirements.

Requirement No 11

[REQ 11] The Host shall:

Maintain a list of points of contact for each client. This point of contact must be able to designate to the Host a healthcare professional authorised to access the DSCPs where necessary;
Be able to transmit this list without delay to the competent authority upon request, in particular in the event of suspension or withdrawal of certification.

.

Requirement No 12

[REQ 12] The Host must communicate to its clients:

A copy of the HDS certificate of conformity. This copy constitutes a guarantee for the Host's Client that compliance requirements have been met;
The certificate of its processors participating in the hosting activity when they are HDS certified.

5.4.5. Documented information

The requirements set out in Chapter 7.5 of ISO 27001 shall apply.

5.5. Operation

5.5.1. Operational planning and control

The requirements set out in Chapter 8.1 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 13

[REQ 13] The Host must plan and control the distribution of information security responsibilities between the Host and its client.

5.5.2. Risk assessment

The requirements set out in paragraph 8.2 of ISO 27001 shall apply.

5.5.3. Risk treatment

The requirements set out in Chapter 8.3 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 14

[REQ 14] In the event of recourse to a certified processor for the performance of all or part of the hosting service, the Host shall provide for a procedure to regulate the risk of loss or suspension of the certification of the processor.

5.6. Performance evaluation

5.6.1. Monitoring, measurement, analysis and evaluation

The requirements set out in Chapter 9.1 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 15

[REQ 15] The Host must allow the client to carry out the following checks on the proposed level of security:

If the Host provides the client with specific resources, the client can carry out or commission technical security audits on these specific resources only. The organisation assists the client or its mandated stakeholder in maintaining information security during these audits;
At the client's request, the Host must provide a management summary of a technical audit report on the resources shared as part of the service. This audit must be carried out by an independent auditor and be less than 3 years old;
The Host must allow the client to consult the traces of access to the DSCP carried by specific resources or to said resources by personnel under its control;
The Host must define the procedures enabling its client to consult its latest HDS certification audit report.

5.6.2. Internal audit

5.6.2.1. General points

The requirements set out in Chapter 9.2.1 of ISO 27001 shall apply taking into account the following requirement.

Requirement No 16

[REQ 16] Internal audits carried out by the Host must include at least:

An audit to determine whether the ISMS complies with the requirements of this framework and is effectively implemented and maintained;
An audit of the traces of access by persons operating on behalf of the organisation to the DSCPs or the systems used for their processing.

5.6.2.2. Internal audit programme

The requirements set out in Chapter 9.2.2 of ISO 27001 shall apply.

5.6.3. Management review

The requirements set out in Chapter 9.3 of ISO 27001 shall apply.

5.7. Improvement

The requirements set out in Chapter 5.10 of ISO 27001 shall apply.

6. REQUIREMENTS RELATING TO THE CONTRACTUAL RELATIONSHIP

The Host is required to provide its client with a model contract in accordance with the regulatory requirements.

NOTE - In particular, it is recommended that the Host, who acts as its client's processor, refer to the model contractual clauses proposed by the European Commission to include in the contract the clauses required under Article 28 of the GDPR (L_2021199EN.01001801.xml (europa.eu)

6.1. Certificate of conformity

Requirement No 17

[REQ 17] In accordance with Article R.1111-11(1) of the CSP, the hosting contract concluded between the Host and its Client must contain a clause mentioning the scope of the certificate of conformity obtained by the Host, as well as its dates of issue and renewal.

6.2. Description of the services performed

Requirement No 18

[REQ 18] In accordance with Article R.1111-11(2) of the CSP, the hosting contract concluded between the Host and its Client must include a clause relating to the description of the services provided, including the content of the services and expected results, in particular for the purpose of guaranteeing the availability, integrity, confidentiality and auditability of the data hosted.

6.3. Respecting the rights of data subjects

Requirement No 19

[REQ 19] In accordance with Article R.1111-11(4) of the CSP, the hosting contract concluded between the Host and its Client must contain a clause relating to the measures implemented to guarantee the respect of the rights of the health data subjects. This clause must include the following particulars: the procedures for exercising the rights of access,

rectification, limitation, opposition, erasure and portability of data (where applicable), the procedures for reporting a personal data breach to the data controller, the procedures for conducting audits by the Data Protection Officer.

6.4. Appointment of a contractual referent

Requirement No 20

[REQ 20] In accordance with Article R.1111-11(5) of the CSP, the hosting contract concluded between the Host and its Client must contain a clause mentioning the contractual referent of the client of the Host to be contacted for the handling of incidents having an impact on the hosted health data.

6.5. Quality and performance indicators

Requirement No 21

[REQ 21] In accordance with Article R.1111-11(6) of the CSP, the hosting contract concluded between the Host and its Client must include a clause specifying the quality and performance indicators enabling the verification of the level of service announced, the guaranteed level, the periodicity of their measurement, as well as the existence or absence of penalties applicable to non-compliance with these indicators.

6.6. Use of subcontracting

Requirement No 22

[REQ 22] In accordance with Article R. 1111-11(7) of the CSP, the hosting contract concluded between the Host and its Client must provide for information on the conditions for the use of any external technical service providers and the commitments made by the Host to ensure that such use ensures an equivalent level of guarantee protection with regard to the obligations incumbent on the Host, in compliance with Article 28.4 of the GDPR.

6.7. Access to hosted personal health data

Requirement No 23

[REQ 23] In accordance with Article R.1111-11(8) of the CSP, the hosting contract concluded between the Host and its Client must describe the methods used to regulate access to hosted personal health data.

6.8. Changes or technical developments

Requirement No 24

[REQ 24] In accordance with Article R. 1111-11(9) of the CSP, the hosting contract must specify the obligations of the Host towards its Client in the event of changes or technical developments introduced by it or imposed by the applicable legal framework.

The hosting contract must also provide for the prior agreement of the Client in the event that these changes or developments introduced by the Host do not comply with:

The levels of service as required in the chapter; 6.5.
The guarantees defined in Chapters 6.2 and.6.9.

6.9. Guarantees

Requirement No 25

[REQ 25] In accordance with Article R.1111-11(10) of the CSP, the hosting contract concluded between the Host and its Client must provide for information on the guarantees and procedures put in place by the Host to cover any possible failure on its part.

6.10. Prohibition related to the processing of hosted data

Requirement No 26

[REQ 26] In accordance with Article R.1111-11(11) of the CSP, the hosting contract concluded between the Host and its Client must recall the prohibition for the Host to use the hosted health data for purposes other than the execution of the activity of hosting health data.

6.11. Reversibility

Requirement No 27

[REQ 27] In accordance with Article R.1111-11(12) to (14) of the CSP, a clause relating to reversibility must set out the terms and conditions thereof at the end of the service or in the event of early termination of the service for whatever reason, with at least:

A commitment to return all the information entrusted under the service;
A commitment to destroy all copies of this information once it has been returned;
The procedures for calculating the costs and deadlines for returning copies;
The formats in which health data can be returned, read and used for the purpose of portability, and, where applicable, the modalities for moving virtual machines/containers.

7. DATA SOVEREIGNTY

Requirement No 28

[REQ 28] Whichever DSCP hosting activity is offered to the Client by the Host or one of its processors, and provided that it involves storage of DSCPs, then the Host or its processors must store these DSCPs exclusively within the European Economic Area (EEA), without prejudice to the cases of remote access referred to in Requirement No 29. The Host shall document and communicate to the Client the location of this storage.

Requirement No 29

[REQ 29] Where the service offered by the Host or one of its processors involves remote access from a country which is not part of the European Economic Area (EEA), such access must be based on a adequacy decision by the Commission adopted pursuant to Article 45 of the GDPR[1] or, failing that, on one of the appropriate guarantees provided for in Article 46 of the Regulation.

In the latter case, the host shall inform its client of the absence of an adequacy decision, on the one hand, and of the appropriate safeguards within the meaning of Article 46 of the GDPR put in place to regulate this remote access, on the other hand.

> The host shall inform the client and document the appropriate safeguards put in place, and where applicable, any other measures to ensure a level of data protection equivalent to that guaranteed by European Union law.

With regard to the additional measures referred to in Requirement No 29, the host should take into account the recommendations of the European Data Protection Board 01/2020 on measures to supplement the transfer instruments designed to ensure compliance with the EU level of protection of personal data (version 2.0, adopted on 18 June 2021).

Requirement No 30

[REQ 30] When the Host, or one of its processors involved in the hosting service, is subject to the legislation of a third country which does not provide an adequate level of protection within the meaning of Article 45 of the GDPR, the Host must indicate in the contract which binds it to its client and inform the awarding body:

- The list of non-European regulations under which the Host, or one of its processors involved in the hosting service, would be required to allow unauthorised access by Union law to the DSCPs within the meaning of Article 48 of the GDPR;
- The measures implemented by the Host to mitigate the risks of unauthorised access to DSCPs induced by these non-European regulations;
- A description of the residual risks of unauthorised access to DSCPs through non-European regulations that would remain despite these measures.

[1] The list of countries ensuring an adequate level of protection can be found on the CNIL website: www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

With respect to these measures implemented to mitigate the access risks referred to in Requirement No 30, the host shall take into account the guidelines of the European Data Protection Board 01/2020 on measures to supplement transfer instruments to ensure compliance with the EU level of protection of personal data (version 2.0, adopted on 18 June 2021).

Requirement No 31

[REQ 31] The Host shall make public and update the mapping of transfers of DSCPs to a country outside the European Economic Area, including any remote access referred to in Requirement No 29 as well as the description of risks of unauthorised access covered by Requirement No 30. The arrangements for informing the public must take the following form:

- If the certified activity is SecNumCloud qualified (version 3.2), the Host must provide the following information: " No risk of access imposed by the legislation of a third country in breach of EU law";

- If the certified activity does not benefit from a SecNumCloud qualification (version 3.2) and does not involve a transfer of DSCP to a country outside the European Economic Area, the Host must provide the following information: " No transfer of personal health data to a country outside the European Economic Area";

- If the certified activity does not benefit from a SecNumCloud qualification (version 3.2) and includes one or more transfers of DSCPs to a country outside the European Economic Area or a risk of unauthorised access covered by Requirement no 30, the Host must provide the information in the table provided in Chapter 8.

The Host must make this information available to the public in a legible manner on a dedicated page of an accessible website and communicate the URL of the page to the awarding body. This URL shall be published in the list of certified hosts on the ANS website.

8. REPRESENTATION OF GUARANTEES

The purpose of this chapter is to provide clients of Health Data Hosts with greater transparency regarding the scope of the service covered by HDS certification. It enables clients of a service to find out about the various players on which their service provider relies to deliver its service.

Thus, this standard representation is used to list the players involved in the processing of DSCPs in the context of the proposed hosting service.

Business name of the actor	Role in the hosting service (Host/processor of the Host)	HDS certified (yes/no/exempted)	SecNumCloud 3.2 qualified	Hosting activities in which the player is involved	Access to personal health data from countries outside the European Economic Area, by the Host or one of its processors (Requirement No 29 of the HDS framework)	Host or processor subject to a risk of access to personal health data from countries outside the European Economic Area, imposed by the legislation of a third country in breach of EU law (Requirement no 30 of the HDS framework)
	□ Host □ Processor	□ Yes □ No □ Exempted	□ Yes, no risk of unauthorised access to data covered by HDS framework Requirement No 30 □ No		□ Yes □ No, no access to data from a country outside the European Economic Area If yes, specify the country concerned: -covered by an adequacy decision within the meaning of Article 45 of the GDPR: XX (specify country) - not covered by an adequacy decision within the meaning of Article 45 of the GDPR: XX (specify country)	□ Yes □ No If yes, specify the country concerned:

9. SUMMARY OF REQUIREMENTS

Requirement No 01

[REQ 01] The certification of a Host requires:

That it has implemented an Information Security Management System (ISMS) certified in accordance with the ISO 27001 standard, supplemented by the requirements defined in Chapter 5.;
Whereas the scope of this ISMS covers all the Host's health data hosting activities;
Contracts concluded with its clients meet the requirements set out in Chapter6.;
That it complies with the sovereignty requirements defined in Chapter 7;
That it communicates to its clients the presentation of the guarantees formalised in accordance with the Chapter.

Requirement No 02

[REQ 02] In determining its external and internal issues, the Host must take into account the fact that its mission requires it to protect the DSCPs entrusted to it by its clients.

Requirement No 03

[REQ 03] In determining the requirements of parties concerned, the Host must take into account the applicable legal framework for the protection of DSCP.

Requirement No 04

[REQ 04] The scope of the ISMS must include all DSCP processing provided by the Host. It must cover all the means and processes of processing DSCPs, including backups and transfers of material information media.

Requirement No 05

[REQ 05] When assessing risks, the Host must at least consider the following events:

A. Failure of material information media due to physical and environmental threats.
B. Loss of control of material information media, in particular during:
    a. Copying DSCPs on portable media;
    b. Any materialisation in paper format;
    c. Reallocation of storage spaces.
C. Damage, compromise or interruption of an internal or external information flow under the responsibility of the Host.
D. Failure to control the access granted, whether to staff under the control of the organisation or to

those designated by its clients:

a. Allocation, modification and withdrawal of access rights;
b. Distribution of electronic identification means;
c. Traceability and accountability of access;
d. Occasional access during audits and intrusion tests.

E. Failure to control interventions, whether at the initiative of the organisation or commissioned by a client.
F. Unforeseen use of the service due to clumsiness or malicious intent.
G. Hardware or software failures, with inability to meet business continuity or recovery commitments.
H. Subjection of the Host or any processors to non-European legislation which may result in a breach of the DSCP.

Requirement No 06

[REQ 06] Where subcontracting is used, the Host must ensure that it controls changes to the technical and organisational measures of its processors to deal with the identified risks.

Requirement No 07

[REQ 07] In order to reduce the risk of unforeseen use of the system, the Host must ensure that:

The interfaces offered to clients are available at least in French;
The first level support is at least in French. .

Requirement No 08

[REQ 08] The declaration of applicability must be available in French to auditors on request.

Requirement No 09

[REQ 09] The information security objectives established by the Host must include the protection of DSCPs entrusted to it by its clients and include compliance with the obligations of the GDPR.

Requirement No 10

[REQ 10] Staff working for the Host must be made aware of the criticality in terms of availability, confidentiality and integrity of hosted DSCPs.

This requirement also applies to the staff of any processors of the Host.

Requirement No 11

[REQ 11] The Host shall:

Maintain a list of points of contact for each client. This point of contact must be able to designate to the Host a healthcare professional authorised to access the DSCPs where necessary.
Be able to transmit this list without delay to the competent authority upon request, in particular in the event of suspension or withdrawal of certification.

.

Requirement No 12

[REQ 12] The Host must communicate to its clients:

A copy of the HDS certificate of conformity. This copy constitutes a guarantee for the Host's Client that compliance requirements have been met;
The certificate of its processors participating in the hosting activity when they are HDS certified.

Requirement No 13

[REQ 13] The Host must plan and control the distribution of information security responsibilities between the Host and its client.

Requirement No 14

[REQ 14] In the event of recourse to a certified processor for the performance of all or part of the hosting service, the Host shall provide for a procedure to regulate the risk of loss or suspension of the certification of the processor.

Requirement No 15

[REQ 15] The Host must allow the client to carry out the following checks on the proposed level of security:

If the Host provides the client with specific resources, the client can carry out or commission technical security audits on these specific resources only. The organisation assists the client or its mandated stakeholder in maintaining information security during these audits;
At the client's request, the Host must provide a management summary of a technical audit report on the resources shared as part of the service. This audit must be carried out by an independent auditor and be less than 3 years old;
The Host must allow the client to consult the traces of access to the DSCP carried by specific resources or to said resources by personnel under its control;
The Host must define the procedures enabling its client to consult its latest HDS certification audit report.

Requirement No 16

[REQ 16] Internal audits carried out by the Host must include at least:

An audit to determine whether the ISMS complies with the requirements of this framework and is effectively implemented and maintained;
An audit of the traces of access by persons operating on behalf of the organisation to the DSCPs or the systems used for their processing.

Requirement No 17

[REQ 17] In accordance with Article R.1111-11(1) of the CSP, the hosting contract concluded between the Host and its Client must contain a clause mentioning the scope of the certificate of conformity obtained by the Host, as well as its dates of issue and renewal.

Requirement No 18

[REQ 18] In accordance with Article R.1111-11(2) of the CSP, the hosting contract concluded between the Host and its Client must include a clause relating to the description of the services provided, including the content of the services and expected results, in particular for the purpose of guaranteeing the availability, integrity, confidentiality and auditability of the data hosted.

Requirement No 19

[REQ 19] In accordance with Article R.1111-11(4) of the CSP, the hosting contract concluded between the Host and its Client must contain a clause relating to the measures implemented to guarantee the respect of the rights of the health data subjects. This clause must include the following particulars: the procedures for exercising the rights of access, rectification, limitation, opposition, erasure and portability of data (where applicable), the procedures for reporting a personal data breach to the data controller, the procedures for conducting audits by the Data Protection Officer.

Requirement No 20

[REQ 20] In accordance with Article R.1111-11(5) of the CSP, the hosting contract concluded between the Host and its Client must contain a clause mentioning the contractual referent of the client of the Host to be contacted for the handling of incidents having an impact on the hosted health data.

Requirement No 21

[REQ 21] In accordance with Article R.1111-11(6) of the CSP, the hosting contract concluded between the Host and its Client must include a clause specifying the quality and performance indicators enabling the verification of the level of service announced, the guaranteed level, the periodicity of their measurement, as well as the existence or absence of penalties applicable to non-compliance with these indicators.

Requirement No 22

[REQ 22] In accordance with Article R. 1111-11(7) of the CSP, the hosting contract concluded between the Host and its Client must provide for information on the conditions for the use of any external technical service providers and the commitments made by the Host to ensure that such use ensures an equivalent level of guarantee protection with regard to the obligations incumbent on the Host, in compliance with Article 28.4 of the GDPR.

Requirement No 23

[REQ 23] In accordance with Article R.1111-11(8) of the CSP, the hosting contract concluded between the Host and its Client must describe the methods used to regulate access to hosted personal health data.

Requirement No 24

[REQ 24] In accordance with Article R. 1111-11(9) of the CSP, the hosting contract must specify the obligations of the Host towards its Client in the event of changes or technical developments introduced by it or imposed by the applicable legal framework.

The hosting contract must also provide for the prior agreement of the Client in the event that these changes or developments introduced by the Host do not comply with:

The levels of service as required in the chapter; 6.5.
The guarantees defined in Chapters 6.2 and 6.9.

Requirement No 25

[REQ 25] In accordance with Article R.1111-11(10) of the CSP, the hosting contract concluded between the Host and its Client must provide for information on the guarantees and procedures put in place by the Host to cover any possible failure on its part.

Requirement No 26

[REQ 26] In accordance with Article R.1111-11(11) of the CSP, the hosting contract concluded between the Host and its Client must recall the prohibition for the Host to use the hosted health data for purposes other than the execution of the activity of hosting health data.

Requirement No 27

[REQ 27] In accordance with Article R.1111-11(12) to (14) of the CSP, a clause relating to reversibility must set out the terms and conditions thereof at the end of the service or in the event of early termination of the service for whatever reason, with at least:

A commitment to return all the information entrusted under the service;
A commitment to destroy all copies of this information once it has been returned;
The procedures for calculating the costs and deadlines for returning copies;
The formats in which health data can be returned, read and used for the purpose of portability, and, where applicable, the modalities for moving virtual machines/containers.

Requirement No 28

[REQ 28] Whichever DSCP hosting activity is offered to the Client by the Host or one of its processors, and provided that it involves storage of DSCPs, then the Host or its processors must store these DSCPs exclusively within the European Economic Area (EEA), without prejudice to the cases of remote access referred to in Requirement No 29. The Host shall document and communicate to the Client the location of this storage.

Requirement No 29

[REQ 29] Where the service offered by the Host or one of its processors involves remote access from a country which is not part of the European Economic Area (EEA), such access must be based on a adequacy decision by the Commission adopted pursuant to Article 45 of the GDPR[2] or, failing that, on one of the appropriate guarantees provided for in Article 46 of the Regulation.

In the latter case, the host shall inform its client of the absence of an adequacy decision, on the one hand, and of the appropriate safeguards within the meaning of Article 46 of the GDPR put in place to regulate this remote access, on the other hand.

The host shall inform the client and document the appropriate safeguards put in place, and where applicable, any other measures to ensure a level of data protection equivalent to that guaranteed by European Union law.

Requirement No 30

[REQ 30] When the Host, or one of its processors involved in the hosting service, is subject to the legislation of a third country which does not provide an adequate level of protection within the meaning of Article 45 of the GDPR, the Host must indicate in the contract which binds it to its client and inform the awarding body:

[2] The list of countries ensuring an adequate level of protection can be found on the CNIL website: www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

- The list of non-European regulations under which the Host, or one of its processors involved in the hosting service, would be required to allow unauthorised access by Union law to the DSCPs within the meaning of Article 48 of the GDPR;
- The measures implemented by the Host to mitigate the risks of unauthorised access to DSCPs induced by these non-European regulations;
- A description of the residual risks of unauthorised access to DSCPs through non-European regulations that would remain despite these measures
- .

Requirement No 31

[REQ 31] The Host shall make public and update the mapping of transfers of DSCPs to a country outside the European Economic Area, including any remote access referred to in Requirement no 29 as well as the description of risks of unauthorised access covered by Requirement no 30. The arrangements for informing the public must take the following form:

- If the certified activity is SecNumCloud qualified (version 3.2), the Host must provide the following information: “no risk of access imposed by the legislation of a third country in breach of EU law”

- If the certified activity does not benefit from a SecNumCloud qualification (version 3.2) and does not involve a transfer of DSCP to a country outside the European Economic Area, the Host must provide the following information: “No transfer of personal health data to a country outside the European Economic Area”;

- If the certified activity does not benefit from a SecNumCloud qualification (version 3.2) and includes one or more transfers of DSCPs to a country outside the European Economic Area or a risk of unauthorised access covered by Requirement no 30, the Host must provide the information in the table provided in Chapter 8.

The Host must make this information available to the public in a legible manner on a dedicated page of an accessible website and communicate the URL of the page to the awarding body. This URL shall be published in the list of certified hosts on the ANS website.

Annex 1: Correspondence matrix with SecNumCloud

The matrix below explains the correspondence between each measure in Annex A of ISO 27001 and the requirements chapter of the SecNumCloud v3.2 framework. Note that the correspondence does not mean that there is an equivalence between an ISO 27001 measure and a SecNumCloud 3.2 requirement.

The effectiveness of the measures remains to be assessed for HDS certification.

Measure Annex A	Applicable SecNumCloud Requirements
5.1 – Information security policies	5.2 – Information security policy

Measure Annex A	Applicable SecNumCloud Requirements
5.2 – Functions and responsibilities related to information security	6.1 – Functions and responsibilities related to information security.
5.3 – Separation of duties	6.2 – Separation of duties
5.4 – Management responsibilities	No related requirement
5.5 – Contacts with the authorities	6.3 – Relations with the authorities
5.6 – Contacts with specific interest groups	6.4 – Relations with special interest groups
5.7 – Threat monitoring	No related requirement
5.8 – Information security in project management	6.5 – Information security in project management
5.9 – Inventory of information and other associated assets	8.1 – Inventory and ownership of assets
5.10 – Correct use of information and other associated assets	8.4 – Information labelling and handling
5.11 – Return of assets	8.2 – Return of assets
5.12 – Classification of information	8.3 - Identification

Measure Annex A	Applicable SecNumCloud Requirements
5.13 – Information marking	8.4 – Information labelling and handling
5.14 – Transfer of information	10.2 – Flow encryption
5.15 – Access control	9.1 – Access policies and control
5.16 – Identity management	9.2 – User registration and unsubscription
5.17 – Authentication information	10.3 – Hashing passwords
5.18 – Access rights	9.2 – User registration and unsubscription 9.4 – Review of user access rights
5.19 – Information security in supplier relationships	15.1 – Identification of third parties
5.20 – Information security in supplier agreements	15.2 – Security in third-party agreements 15.5 – Confidentiality commitments
5.21 – Information security management in the information and communication technology (TIC) supply chain	15.1 – Identification of third parties 15.3 – Monitoring and review of third party services
5.22 – Monitoring, review and management of changes in supplier services	15.3 – Monitoring and review of third party services
5.23 – Information security in the use of cloud services	15.1 – Identification of third parties 15.3 – Monitoring and review of third party services 19.6 – Immunity from non-EU law (d)

Measure Annex A	Applicable SecNumCloud Requirements
5.24 – Planning and preparation of the management of information security incidents	16.1 – Responsibilities and procedures
5.25 – Information security event assessment and decision-making	16.3 – Assessment of information security events and decision-making
5.26 – Response to information security incidents	16.4 – Response to incidents related to information security
5.27 – Learning from information security incidents	16.5 – Learning from incidents related to information security
5.28 – Collection of evidence	16.6 – Gathering evidence
5.29 – Information security during disruption	No related requirement
5.30 – Preparing TICs for business continuity	17.4 – Availability of information processing resources
5.31 – Legal, statutory, regulatory and contractual requirements	18.1 – Identification of applicable legislation and contractual requirements
5.32 – Intellectual property rights	No related requirement
5.33 – Protection of records	No related requirement
5.34 – Protection of privacy and personal data (DCP)	19.5 – Personal data protection

Measure Annex A	Applicable SecNumCloud Requirements
5.35 – Independent audit of information security	18.2 – Independent review of information security
5.36 – Compliance with information security policies, rules and standards	18.3 – Compliance with security policies and standards 18.4 – Technical compliance examination
5.37 – Documented operating procedures	12.1 – Documented operating procedures
6.1 – Selection of candidates	7.1 – Selection of candidates
6.2 – Terms and conditions of employment	7.2 – Terms of employment
6.3 – Information security awareness, education, and training	7.3 – Information security awareness, education, and training
6.4 – Disciplinary process	7.4 – Disciplinary process
6.5 – Responsibilities after termination or change of employment	7.5 – Breach, termination, or amendment of employment contract
6.6 – Confidentiality or non-disclosure agreements	15.5 – Confidentiality commitments
6.7 – Remote working	12.12 – Administration (c) 12.13 – Remote diagnosis and remote maintenance of infrastructure components
6.8 – Reporting of information security events	16.2 – Alerts related to information security

Measure Annex A	Applicable SecNumCloud Requirements
7.1 – Physical security perimeters	11.1 – Physical security perimeters
7.2 – Physical inputs	11.2 – Physical access control 11.5 – Delivery and loading areas
7.3 – Securing offices, rooms and equipment	No related requirement
7.4 – Physical security monitoring	11.2.1 – Private areas (h) 11.2.2 – Sensitive areas (h)
7.5 – Protecting against external and environmental threats	11.3 – Protecting against external and environmental threats
7.6 – Work in secure areas	11.4 – Work in private and sensitive areas
7.7 – Clean desk and empty screen	No related requirement
7.8 – Location and protection of equipment	11.10 – Equipment awaiting use
7.9 – Security of off-premises assets	No related requirement
7.10 – Storage media	11.8 – Removal of assets
7.11 – Support services	11.3 – Protecting against external and environmental threats 11.7 – Maintenance of equipment

Measure Annex A	Applicable SecNumCloud Requirements
7.12 – Cabling security	11.6 – Cabling security
7.13 – Equipment maintenance	11.7 – Maintenance of equipment
7.14 – Safe disposal or recycling of equipment	11.9 – Secure recycling of equipment
8.1 – End-user terminals	12.12 - Administration
8.2 – Privileged access rights	9.3 – Management of access rights
8.3 – Restriction of access to data	9.7 – Restriction of access to data
8.4 – Access to source codes	No related requirement
8.5 – Secure authentication	9.5 – Managing user authentications
8.6 – Sizing	No related requirement
8.7 – Protection against malware	12.4 – Measures against malicious code
8.8 – Management of technical vulnerabilities	12.11 – Management of technical vulnerabilities

Measure Annex A	Applicable SecNumCloud Requirements
8.9 – Configuration management	18.2.1 – Initial review 18.2.2 – Review of major changes
8.10 – Deletion of information	11.9 – Secure recycling of equipment 19.4 – End of contract
8.11 – Masking data	No related requirement
8.12 – Prevention of data leakage	12.14 – Monitoring infrastructure outflows 19.6 – Immunity to non-EU law
8.13 – Information backup	12.5 – Information backup 17.5 – Backup of the configuration of the technical infrastructure 17.6 – Provision of a back-up system of the sponsor's data
8.14 – Redundancy of data processing resources	17.1 – Organisation of business continuity 17.2 – Implementation of business continuity 17.3 – Verifying, reviewing and assessing business continuity
8.15 – Logging	12.6 – Event logging 12.7 – Protection of logged information 12.9 – Analysis and correlation of events
8.16 – Monitoring activities	13.3 – Network monitoring
8.17 – Clock synchronisation	12.8 – Clock synchronisation
8.18 – Use of privileged utilities	No related requirement
8.19 – Installing software on operational systems	12.10- Installing software on systems in operation

Measure Annex A	Applicable SecNumCloud Requirements
8.20 – Network security	13.1 – Mapping of the information system 13.2 – Network partitioning
8.21 – Security of network services	9.6 – Access to administration services 13.2 – Network partitioning (d,e)
8.22 – Network partitioning	13.2 – Network partitioning
8.23 – Web filtering	13.2 – Network partitioning (c)
8.24 – Use of cryptography	10.4 – Non-repudiation 10.5 – Secrets management 10.6 – Roots of trust
8.25 – Secure development life cycle	14.1 – Secure development policy
8.26 – Application security requirements	5.3 – Risk assessment
8.27 – Engineering and architecture principles for secure systems	No related requirement
8.28 – Secure coding	18.2.2 – Initial review 18.2.3 – Review of major changes
8.29 – Security testing in development and acceptance	14.6 – Security testing and system compliance
8.30 – Outsourced development	14.5 – Outsourced development
8.31 – Separation of development, testing and operational environments	12.3 – Separation of development, testing and operating environments

Measure Annex A	Applicable SecNumCloud Requirements
	14.4 – Secure development environment
8.32 – Change management	12.2 – Change management 14.2 – System change control procedures 14.3 – Technical review of applications following changes to the operating platform
8.33 – Test information	14.7 – Protection of test data
8.34 – Protection of information systems during audit tests	No related requirement

Two SecNumCloud requirements are not correlated to ISO 27001 reference measures, but are partially found in the contractual or additional ISMS requirements:

- Requirements concerning the content of the service agreement (19.1 of SecNumCloud);
- Data localisation requirement (19.2 of SecNumCloud).

AGENCE DU NUMÉRIQUE EN SANTÉ

HDS Accreditation framework

Status: Under validation | *Classification: Public* | *Version: v2023 – to be validated*

Agence du Numérique en Santé (Digital Health Agency)
2-10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Reference documents

Reference no 1: NF EN ISO/IEC 17021-1:2015

Conformity assessment -- Requirements for bodies auditing and certifying management systems

Reference no 2: NF ISO/IEC 27001:2022

Information security, cybersecurity and privacy – Information security management systems - Requirements

Reference no 3: HDS certification framework requirements v2023

Reference no 4: IAF MD1 version in force

IAF requirements document for multi-site certification by sampling

Reference no 5: IAF MD2 version in force

IAF requirements document for transfer of management system certification under accreditation

Reference no 6: IAF MD4 version in force

IAF requirements document for the use of Computer-Assisted Audit Techniques ("CAAT") for accredited management system certification

Reference no 7: IAF MD5 version in force

Determining the audit time of quality management systems and environmental management systems

Reference no 8: IAF MD11 version in force

IAF requirements document for the application of ISO/IEC 17021 for Integrated Management System (IMS) audits

The IAF requirements documents are available on the IAF website.

CONTENTS

10. INTRODUCTION

10.1. Purpose of the document

This document is intended for certification bodies wishing to be accredited for the certification of Health Data Hosts. It describes the accreditation process for certification bodies and the certification process for hosts.

10.2. Structure of the document

This document is organised in seven parts and two annexes:

- introduction of the document;
- description of the scope of the accreditation framework;
- description of the standards applicable within the accreditation framework;
- list of acronyms used in the accreditation framework;
- description of the conditions, criteria and procedures for accreditation of certification bodies;
- definition of the responsibilities of accreditation bodies;
- description of the conditions, criteria and procedures for certification of hosts.

Annexes

- Annex A setting out the necessary elements to determine the audit duration for HDS certification;
- Annex B setting out the templates of documents to be used by certification bodies to send information to the competent authority.
- .

10.2.1. Definitions

10.2.1.1. Actor

Any stakeholder contributing to the security of personal health data, excluding the data controller and processors of a certified Host when they act in accordance with the security policy and under the supervision of the said Host

10.2.1.2. Administration and operation of the information system containing health data

The activity of administration and operation of the information system containing health data consists in mastering the interventions on the resources made available to the client of the Host. It includes all of the following ancillary activities:

- the definition of a process for the allocation and annual review of nominative, justified and necessary access rights;
- securing the access procedure;
- the collection and preservation of traces of the accesses made and the reasons for them;
- prior validation of interventions (intervention plan, intervention process).

The validation of interventions consists in ensuring that they do not degrade the security of the hosted information either for the client concerned or for the other clients of the Host. This validation may be carried out in the following cases:

- a priori, for interventions that the client could carry out independently;
- when requesting service from the Host.

The definition of the allocation process, security, collection and validation are intrinsic and compulsory to the activities defined in 1 to 4 of Article R. 1111-9 of the Public Health Code. If they are carried out solely insofar as they are related and consubstantial to activities 1 to 4, the Host is not required to be certified for Activity 5. It shall only be required to be so in the event that it only carries out Activity 5.

10.2.1.3. Client of the Host

The client of the Host (also referred to as “client”) designates the natural or legal person who subscribes to the service provided by the Host.

10.2.1.4. Host

The Host, also referred to as the organisation in the ISO 27001 standard, is the applicant for certification as Host of health data or for renewal of its certification. It provides all or part of a hosting service for personal health data (or “health data”).

10.2.1.5. Electronic identification means

An electronic identification means is a tangible or intangible element containing personal identification data and used to authenticate to an online service.

10.2.1.6. Data controller

The controller within the meaning of Regulation 2016/679 designates the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing.

11. SCOPE

11.1. Applicability of the HDS certification framework

The scope of the framework shall be defined by Articles L. 1111-8, R. 1111-8-8 and R. 1111-9 of the Public Health Code.

11.1.1. Role of Host

HDS certification shall apply to any natural or legal person who provides all or part of a hosting service for personal health data and who is a processor within the meaning of Article 28 of the GDPR.

11.1.2. Nature of the data

The hosted data must be personal data relating to health, as defined in Article 4.15 of the GDPR.

11.1.3. Context of the collection

The HDS certification concerns personal health data collected during prevention, diagnosis, care or social or medico-social follow-up activities.

These personal health data must be hosted on behalf of:

the natural or legal persons responsible for the production or collection of the data;

or the patient himself.

11.1.4. Activities carried out

Article R. 1111-9 of the CSP defines the activity of hosting health data.

The provision of all or some of the following activities on behalf of the data controller as mentioned in I(1) of Article R. 1111-8-8 or of the patient as mentioned in I(2) of the same Article shall be considered to be hosting personal health data in digital format as defined in Article L. 1111-8(II):

1. The provision and maintenance in operational condition of physical sites for hosting the hardware infrastructure of the information system used to process the health data;

2. The provision and maintenance in operational condition of the hardware infrastructure of the information system used to process the health data;

3. The provision and maintenance in operational condition of the virtual infrastructure of the information system used to process the health data;

4. The provision and maintenance in operational condition of the platform for hosting information system applications;

5. The management and operation of the information system containing the health data;

6. Backing up health data.

Activity 5 is specified in paragraph 2.1.2.

Data backup Activity 6 should be interpreted as including only outsourced backups. The backups inherently necessary for Activities 1 to 5 are within the scope of Activities 1 to 5.

12. NORMATIVE REFERENCES

The documents listed below are referenced normatively in this framework and are indispensable for its application.

NF IN ISO 27001:2023, *Information Security, Cybersecurity and Privacy – Information Security Management Systems – Requirements*

NF IN ISO/IEC 17021-1:2015, *Conformity assessment - Requirements for bodies auditing and certifying management systems – Part 1: Requirements*

In the rest of the document, references to these standards will be made as follows:

- NF ISO 27001 for standard NF EN ISO 27001:2023;
- NF ISO 17021-1 for standard NF EN ISO/IEC 17021-1:2015.

13. ACRONYMS USED

COFRAC	Comité Français d'Accréditation (French Accreditation Committee)
DDA	Déclaration d'Applicabilité documentée - Documented statement of applicability describing security objectives, as well as appropriate and applicable measures to an organisation's Information Security Management System
HDS	Hébergeur de Données de Santé (Health Data Host)
IAF	International Accreditation Forum
CEI/IEC	Commission Electrotechnique Internationale/International Electrotechnical Commission
ISO	International Organization for Standardization
OC	Organisme de Certification (Certification body)

14. CONDITIONS, CRITERIA AND PROCEDURES FOR ACCREDITATION

The conditions, criteria and procedures for accreditation are based on the standards of NF ISO 17021-1. Accreditation shall attest to the competence, impartiality and reliability of a body to verify compliance with established and formalised requirements. Accreditation is a so-called second-level check that aims to control how the controller operates.

14.1. Accreditation conditions and criteria

Certification bodies authorised to issue HDS certificates of conformity must be accredited by a national accreditation body as defined in Regulation (EC) 765/2008 (COFRAC in France or its equivalent in other countries signatory to multilateral international recognition agreements) in accordance with this accreditation framework, which will be regularly reviewed in order to incorporate technological developments in health information systems, as well as changes in hosting professions.

The application and compliance with the requirements of the accreditation framework shall ensure that accredited bodies are competent to issue HDS certifications.

Accreditation shall cover the assessment of bodies wishing to be certified as hosts of personal health data.

For a body to be accredited to issue HDS certifications, it must be accredited in accordance with the requirements of NF ISO 17021-1 and apply the rules in force for the audit and certification of information systems security management systems in accordance with ISO 27001. In addition, this accreditation framework defines the specific requirements that apply to HDS certification.

14.2. Accreditation requirements

14.2.1. General requirements

14.2.1.1. Contractual and legal area

The requirements of §5.1 of NF ISO 17021-1 shall apply.

14.2.1.2. Impartiality management

The requirements of §5.2 of NF ISO 17021-1 shall apply.

14.2.1.3. Responsibility and financing

The requirements of §5.3 of NF ISO 17021-1 shall apply.

14.2.2. Structural requirements

14.2.2.1. Competence of staff

The requirements of §7.1 of NF ISO 17021-1 shall apply.

When selecting the audit team, the certification body shall ensure that the skills brought to each assignment are appropriate. The team must have sufficient knowledge of the information security, the hosting of sensitive data and the services offered by health data hosts.

In particular, auditors of the certification body involved in HDS certification activities must be able to demonstrate that they have skills in the field of information system security and in particular health information systems.

The management of the certification body must define the processes and have the necessary resources to enable it to determine whether or not the auditors are competent for the tasks to be performed under the HDS certification. The certification body must be able to communicate to its clients the skills of its staff involved in the certification activities.

14.2.2.2. Staff involved in certification activities

The requirements of §7.2 of NF ISO 17021-1 shall apply.

The team of auditors can be strengthened by technical experts. These technical experts do not replace auditors, but provide them with support on issues relating to adequacy of security and devices used to host health data.

It is recommended that experts have specific skills in the field of health acquired through training or a project.

The certification body must have a procedure enabling to:

- select auditors and technical experts on the basis of their skills, training, qualifications and experience;
- assess the conduct of auditors and technical experts during certification and surveillance audits.

14.2.2.3. Intervention of individual external auditors and technical experts

The requirements of §7.3 of NF ISO 17021-1 shall apply.

14.2.2.4. Staff records

The requirements of §7.4 of NF ISO 17021-1 shall apply.

14.2.2.5. Outsourcing

The requirements of §7.5 of NF ISO 17021-1 shall apply.

14.2.3. Information requirements

14.2.3.1. Publicly available information

The requirements of §8.1 of NF ISO 17021-1 shall apply.

14.2.3.2. Certification documents

The requirements of §8.2 of NF ISO 17021-1 shall apply.

The certification body shall provide each of its certified clients that host personal health data with documents attesting to their certification.

These documents must:

- specify the scope of the certified service in relation to the activities defined in Chapter 2 "Scope", in particular the list of certified activities;
- specify the ISO standards for which the organisation is already certified and meets the requirements in force (NF ISO 27001).
- specify the location (at least the country) of all sites within the scope of certification.

Where an ISO 27001 certification is issued by an OC other than the one issuing the HDS certification, the certificate shall explicitly state that it is valid subject to obtaining a valid ISO 27001 certification for the same scope.

Note

If processors are used, their sites shall not appear on the certificate.

14.2.3.3. Reference to certification and use of trademarks

The requirements of §8.3 of NF ISO 17021-1 shall apply.

14.2.3.4. Confidentiality

The requirements of §8.4 of NF ISO 17021-1 shall apply.

Before any intervention by the audit team, the certifying body must ensure with the applicant that the information to be provided during the audit does not contain any personal health data or any confidential or sensitive data. Where applicable, the certification body and the applicant must define how to access the system to be audited (confidentiality commitment, etc.).

In the event of an inability to audit the information system without access to personal health data or other confidential or sensitive data, the certification body must inform the applicant, a confidentiality agreement must be drawn up and a healthcare professional acting under the responsibility of the client must be informed.

Chapter 8.4.2 of standard NF ISO 17021-1 is completed as follows: personal health data and any other confidential or sensitive data to which the certification body may have access in the context of the audit may not be disclosed or reused by the certification body or by the applicant for certification.

14.2.3.5. Exchange of information with the competent authority

14.2.3.5.1. HDS suspension report

The certification body shall communicate to the competent authority in French or English any decision to suspend the certification of a health data host.

The information below relating to the health data host whose certification has been suspended must be communicated:

- designation or business name of the health data host for which certification has been suspended;
- identifier number of the suspended certificate;
- date of suspension of the certificate;
- reasons for suspending the HDS certification.

The information must be sent electronically using the template proposed in Annex B: Exchange of information between the certification body and the competent authority.

14.2.3.5.2. HDS withdrawal report

The certification body shall communicate to the competent authority in French or English any decision to withdraw the certification of a health data host.

The information below relating to the health data host whose certification has been withdrawn must be communicated:

- designation or business name of the health data host for which certification has been withdrawn;
- identifier number of the withdrawn certificate;
- date of withdrawal of the certificate;
- reasons for withdrawing the HDS certification.

The information must be sent electronically using the template in Annex B: Exchange of information between the certification body and the competent authority.

14.2.3.5.3. HDS client directory

At least once a month, the certification body shall provide the competent authority with a report of valid, suspended and withdrawn certifications. This report, in French or English, must contain the following data for each health data host:

- designation or business name of the health data host;
- identifier number of the certificate;
- scope of the certification (list of activities);
- address of the certified site and, in the case of multi-site certification, indicate the address of the head office, as well as those of all attached sites;
- status of certification (valid, suspended or withdrawn);
- date of certification.
- URL or contact to enable verification of the certificate with the OC.
- URL of the DSCP transfer declaration page in accordance with requirement 31 of the certification framework

The directory must be sent electronically by using the template in Annex B: Exchange of information between the certification body and the competent authority.

14.2.3.5.4. HDS annual report

The requirements of §8.5 of NF ISO 17021-1 shall apply.

Each year, the certification body must provide the competent authority with an annual report in French or English, including:

- an anonymised summary of HDS certifications, audits performed and non-conformities identified.
- a summary of the difficulties encountered in certifying hosting providers and any proposals for changes to the certification and accreditation standards;
- indicators on the HDS certification procedure, such as:
- number of health data hosts in the process of being certified;
- number of health data hosts failing certification;
- number of certification renewals;
- average duration of audits.

The annual report must be sent electronically between 1 and 31 January of the following year, using the template proposed in Annex B: Exchange of information between the certification body and the competent authority.

14.2.4. Certification process requirements

14.2.4.1. Pre-certification activities

14.2.4.1.1. Application for certification

The requirements of §9.1.1 of NF ISO 17021-1 shall apply.

In the case of a certificate transfer, the IAF MD 2 guide shall apply. In addition, the receiving certification body shall inform the competent authority of any certificate transfer and indicate the name of the issuing certification body.

14.2.4.1.2. Review of the application

The requirements of §9.1.2 of NF ISO 17021-1 shall apply.

14.2.4.1.3. Audit programme

The requirements of §9.1.3 of NF ISO 17021-1 shall apply.

Chapter 9.1.3.1 is supplemented by the following requirement: the description of the scope of certification must specify the list of activities listed in chapter 11. for which the applicant is applying for certification in order to determine the type of HDS certification.

14.2.4.1.4. Determination of audit time

The requirements of §9.1.4 of NF ISO 17021-1 shall apply. In addition, the requirements of the IAF MD 4 and MD 5 guides shall apply.

The audit duration shall be determined by applying the method and tables in "Annex A: Audit duration table for HDS certification" of this document.

If, after calculation, the result is not a whole number, the number of days must be rounded to the nearest half day (e.g.: 5.3 audit days become 5.5 audit days, and 5.2 audit days become 5 audit days).

14.2.4.1.5. Multiple sampling

The requirements of §9.1.5 of NF ISO 17021-1 shall apply. In addition, the IAF MD 1 guide shall apply.

14.2.4.1.6. Multiple management systems standards

The requirements of §9.1.6 of NF ISO 17021-1 shall apply, as well as the IAF MD 11 guide.

14.2.4.2. Audit planning

The requirements of §9.2 of NF ISO 17021-1 shall apply.

14.2.4.3. Initial certification

The requirements of §9.3 of NF ISO 17021-1 shall apply.

14.2.4.4. Conducting audits

The requirements of §9.4 of NF ISO 17021-1 shall apply.

Representatives of the Digital Health Agency may attend an audit as observers.

14.2.4.5. Certification decision

The requirements of §9.5 of NF ISO 17021-1 shall apply.

14.2.4.6. Maintaining certification

The requirements of §9.6 of NF ISO 17021-1 shall apply.

The certification is issued for a period of 3 years. Certified hosts must file with the certification body an application for recertification no later than 3 months before the certification expires.

14.2.4.7. Appeals

The requirements of §9.7 of NF ISO 17021-1 shall apply.

14.2.4.8. Complaints

The requirements of §9.8 of NF ISO 17021-1 shall apply.

14.2.4.9. Client records

The requirements of §9.9 of NF ISO 17021-1 shall apply.

14.2.4.10. Management system requirements for certification bodies

14.2.4.10.1. Options

The requirements of §10.1 of NF ISO 17021-1 shall apply.

14.2.4.10.2. Management system requirements in accordance with ISO 9001

The requirements of §10.2 of NF ISO 17021-1 shall apply.

14.2.4.10.3. General management system requirements

The requirements of §10.3 of NF ISO 17021-1 shall apply.

14.2.5. Assessment procedures

Annex B to standard NF ISO 17021-1 shall apply.

15. RESPONSIBILITIES OF ACCREDITATION BODIES

The tasks of the accreditation bodies (COFRAC, in France, and its European counterparts) are to ensure that the bodies they accredit are competent and impartial and that they remain so over time, regardless of the context.

To certify this competence, the accreditation body shall carry out regular assessments of the functioning of these accredited bodies. The assessments consist of a document review as well as an intervention of the assessors as witnesses to an audit to verify both the quality of the procedures and the way in which they are applied.

15.1. Accreditation process

The accreditation process shall comply with NF ISO 17021-1.

If the certification body is already accredited for the NF ISO 17021-1 standard, a major extension of the scope of accreditation to a new domain shall be carried out. This leads to an assessment at the head office of the body and at least to one activity observation.

If the certification body is not already accredited for NF ISO 17021-1, the initial accreditation process shall be applied.

After favourable admissibility of the application for accreditation by the national accreditation body for HDS certification (operational admissibility), certifying bodies in the process of applying for accreditation are authorised to issue certificates for twelve (12) months.

Accreditation must be obtained within a maximum of twelve (12) months from the date of notification of the positive decision on operational admissibility.

If accreditation is not obtained within this period, the certification body shall inform its clients to contact another certification body to obtain a new certificate.

Certificates issued during the twelve (12) months period will have to be reissued under accreditation if they were initially issued under the same conditions as those for issuing accreditation.

The scope of accreditation is expressed as follows:

Subject of certification	Certification reference	Accreditation framework
Information systems security management systems for health data hosts	HDS Certification Requirements Framework (current version)	HDS Accreditation framework (current version)

15.2. Accreditation suspension process

15.2.1. Suspension decision

In the event of suspension of accreditation at the initiative of the accreditation body, the latter shall forthwith inform the certification body and the competent authority thereof, specifying: the name of the certification body, the date of suspension, the reasons for the suspension decision and the date on which accreditation will be withdrawn if the conditions for lifting the suspension are not met.

The suspension decision shall be notified by registered letter with acknowledgement of receipt and shall specify the scope of the suspension of accreditation, the reasons for the decision to suspend the accreditation body and the conditions under which the body may lift the suspension of the accreditation of the certification body.

If the certification body does not submit the replies requested by the accreditation body within the time limits specified in the suspension decision, accreditation shall be withdrawn for certification activities of the personal health data host.

As soon as it receives the decision to suspend its accreditation, the certification body must inform its clients and cease to make any further reference to the accreditation. A body whose accreditation has been suspended may no longer carry out a certification audit or issue decisions on the health data host's certificate.

15.2.2. Lifting of suspension

In the event of suspension at the initiative of the accreditation body, the conditions for lifting the suspension shall be specified in the suspension decision sent to the certification body.

The decision to lift the suspension may only be issued following an on-site assessment by the certification body or the examination by the accreditation body of an internal audit report sent by the certification body. If the report does not provide sufficient evidence to demonstrate compliance with the accreditation requirements, the certification body shall be informed by letter that its suspension can only be lifted on the basis of the results of an on-site assessment. The decision to lift the suspension shall be notified by the accreditation body. A new accreditation certificate indicating the effective date of the lifting of the suspension shall be drawn up and the technical annex setting out the activities for which accreditation has been granted shall be updated. The expiry date of the accreditation is unchanged from the initial accreditation.

The notification of lifting of suspension shall be sent to the competent authority electronically specifying: the name of the certification body, the date of suspension (if applicable), the reasons for the suspension decision and the date on which the suspension was lifted.

In the event of refusal to lift the suspension, the certification body may appeal against the decision to the accreditation body.

15.3. Accreditation withdrawal process

In the event of withdrawal of accreditation, the accreditation body shall inform the certification body and the competent authority without delay of any measure to withdraw accreditation.

The notification of withdrawal shall be sent to the competent authority electronically specifying: the name of the certification body, the date of suspension (if applicable), the reasons for the decision to withdraw accreditation and the date on which the accreditation was withdrawn.

The withdrawal of accreditation shall take effect on the date of notification of withdrawal by the accreditation body. The decision shall be communicated to the certification body by registered letter with acknowledgement of receipt, specifying the reasons for the decision.

The organisation shall be no longer authorised to issue certificates or maintain existing certificates.

The certification body whose accreditation has been withdrawn must cease all activities related to the certification of health data host and immediately inform the competent authority and its clients so that they can contact another certification body accredited for this purpose, in order to transfer the certification held where appropriate.

The accreditation body shall have the possibility to intervene on the certification body's site in order to ensure that activities relating to the certification of health data hosts have been suspended and that the competent authority and clients have been informed.

15.4. Transfer of certification to a new certification body following withdrawal

The new certification body receiving a transfer request must apply the provisions described in §16. of this document. In particular, the IAF MD2 guide shall apply. If it is impossible to obtain the client’s file from the previous body, the client’s application shall be treated as an initial certification. In all cases, it shall be the responsibility of the "receiving" certification body to assess the elements provided and to establish whether the certification cycle can be resumed at the same certification stage as it was with the original certification body.

15.5. Cessation of activity of a certification body

The accreditation body shall inform the competent authority without delay of any announcement of the cessation of activity of a certification body.

The certification body shall also be required to inform the competent authority, as well as the clients concerned as soon as possible, so that they can apply to another certification body accredited for this purpose, in order to transfer the certification held where appropriate.

16. CONDITIONS, CRITERIA AND PROCEDURES FOR CERTIFICATION

16.1. Certification conditions and criteria

An applicant seeking HDS certification will have to meet the requirements of the HDS certification framework and apply for certification to an accredited certification body in accordance with the HDS accreditation framework.

The certification of a host requires:

- that it has implemented an Information Security Management System (ISMS) certified in accordance with the ISO 27001 standard, supplemented with the requirements defined in Chapter 5 of the certification framework;
- that the scope of this ISMS covers all the Host's health data hosting activities;
- that the contracts concluded with its clients meet the requirements defined in Chapter 6 of the certification framework;
- that it complies with the sovereignty requirements defined in Chapter 7 of the certification framework;
- that it communicates to its clients the presentation of the guarantees formalised in accordance with Chapter 8 of the certification framework.

A host that has already obtained an ISO 27001 certification may claim this certification if it meets the conditions set out in Chapter 16.2..

An applicant who already has this certification shall be assessed within the scope of the requirements of the certification framework not covered by the certification. The certification already obtained shall be checked in accordance with the procedures laid down in Chapter 16.2..

The HDS certificate is issued for 3 years: the expiry date may differ from the expiry date of the ISO 27001 certificate.

The HDS certificate shall explicitly state that it is valid subject to a valid ISO 27001 certification for the same scope.

In the contract between the OC and its client, the following particulars must appear:

- The client shall be informed that in case of non-compliance with a requirement of ISO 27001 noted during an HDS audit, this information shall be transmitted to the OC that has certified the client according to ISO 27001.
- The client shall be obliged to immediately inform the OC of any measures to suspend, withdraw, terminate or transfer his ISO 27001 certificate.

These commitments shall be verified during surveillance audits.

16.2. Equivalence

If the applicant wishes to use the certification according to the NF ISO 27001 standard it has already obtained, this certification must meet all of the following conditions:

- the scope of application of the certification available to the host must include the scope for which the applicant applies for HDS certification;
- audit reports: the initial audit report and the certification surveillance audit reports for which equivalence is requested must be provided at the request of the certification body;
- for an applicant with an ISO 27001 certification, the declaration of applicability (DdA) of the organisation's information security management system must explicitly include:
- the detailed justification for any exclusion from ISO 27001 controls;
- the detailed justification for any non-applicable controls;
- the certification must:
- be valid;
- have been issued by a certification body accredited by a national accreditation body as defined in Regulation (EC) No 765/2008 for the issue of such certificates and whose accreditation must be valid (COFRAC in France or its equivalent in other countries signatories to multilateral international recognition agreements);
- not to be subject to a suspension or withdrawal procedure;
- not to be subject to a transfer request.

The above conditions must be checked by the certification body receiving the HDS certification application, which must record the information received (including copies of certificates) and justify the results of this verification by indicating which certification(s) is/are accepted by the OC prior to the initial audit of the applicant.

Certifications obtained according to international standards equivalent to the French standards indicated above may be recognised under the same conditions. These include certifications of compliance with ISO 27001 and ISO 17021 standards in languages other than French.

16.3. Subcontracting

In case of use of processors by the host, the representation of the guarantees described in Chapter 8 of the HD certification framework shall apply.

Annex A: Audit duration table for HDS certification

The audit time table below provides the framework that should be used for HDS certification audit planning by identifying a starting point based on the total number of people working under the control of the organisation for all positions involved in the health data hosting service and adjusting the important factors.

The OC must provide the client with the determination of the audit time and the supporting documents. These form an integral part of the contract and must be made available to the accreditation body on request.

The starting point for determining the audit time of an HDS certification must be based on the actual number of employees involved in the health data hosting service and then can be adjusted for significant factors that apply to the client to be audited.

Number of people involved in the health data hosting service	HDS certification audit duration (step 1 + step 2) A+B		
	(A) Audit duration NF ISO 27001	(B) Duration of audit of requirements outside NF ISO 27001	Total duration of HDS certification audit
0			0.5[3]
1 – 10	5	2	7
11 - 15	6	2	8
16 - 25	7	2	9
26 - 45	8.5	2	10.5
46 - 65	10	3	13
66 - 85	11	3	14
86 - 125	12	3	15
126 - 175	13	3	16
176 - 275	14	3	17
276 - 425	15	3	18
426 - 625	16.5	4	20.5
626 - 875	17.5	4	21.5
876 - 1175	18.5	4	22.5
1176 - 1550	19.5	4	23.5
1551 – 2025	21	4	25

[3] No reduction factor may apply on this line

Number of people involved in the health data hosting service	HDS certification audit duration (step 1 + step 2) A+B		
	(A) Audit duration NF ISO 27001	(B) Duration of audit of requirements outside NF ISO 27001	Total duration of HDS certification audit
2026 – 2675	22	4	26
2676 – 3450	23	4	27
3451 – 4350	24	5	29
4351 – 5450	25	5	30
5451 – 6800	26	5	31
6801 – 8500	27	5	32
8501 - 10700	28	5	33
10700	Follow the progression above	Follow the progression above	Follow the progression above

The HDS audit duration may be adjusted upwards or downwards depending on specific factors according to current best practices for calculating the ISMS audit durations. These factors include the complexity of the ISMS, the nature of the service concerned, the proof of prior implementation of an ISMS, the technological complexity implemented, the use of processors, the nature of any developments and the number of sites. Changes made to the ISMS are a factor to be taken into account when calculating the duration of surveillance and recertification audits.

According to the best practice rules in force for calculating ISMS audit durations, the maximum reduction in the audit duration is 30% and the maximum increase in the audit duration is 100%. These limits apply to the calculation of the HDS audit duration.

Annex B: Exchange of information between the certification body and the competent authority

HDS annual report

Name of certification body	Date: *dd/mm/yyyy*

Summary of HDS certifications, audits performed and non-conformities identified

Summary of the difficulties encountered during HDS certification

Proposals to improve HDS certification

Indicators on the HDS certification procedure

Number of certifications issued	Number of failures	Number of renewals	Number of suspensions	Number of withdrawals	Number of certifications

					transferred
XXXX	*XXXX*	*XXXX*	*XXXX*	*XXXX*	*XXXX*

HDS client directory

Name of certification body: *XXXX*

Date: *dd/mm/yyyy*

Certificate Identifier	Name of health data host	Scope of certification (list of activities)	URL of the DSCP transfer risk declaration page in accordance with Requirement no 31	Address of the sites	Date of certification	Certificate status	Certificate publication URL or OC Contact

esante.gouv.fr

The portal to access all the services and products offered by the digital health agency and keeping up to date with e-health news.

@esante_gouv.fr