AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Health Data Host (HDS) certification framework

Requirements

Statut : Approved | *Classification : Public* | *Version : v2.0*

This document is the English version of Health Data Host (HDS) certification framework – Requirements – version 2.0.

In case of litigation, only the French version shall be considered as authentic, valid and taken into consideration for any purpose of interpretation.

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

Reference documents

Regulations

Renvoi	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
[ARTR 1111-9] à [ART R1111-11]	Articles R1111-9 à 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

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

Revision history

Version	Date	Commentaire
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	March2023	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.
V2.0	April 2024	Revision published by Order of April 2024 26th, approving the accreditation framework of certification bodies and the certification framework for hosting personal health data Minor change : Link to chapter 8 in requirement 01.

SUMMARY

1. PREAMBULE

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. Definitions

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)

Acronym	
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

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.

3.1.3. 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 n° 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 8

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.

5.4. Context of the organisation

5.4.1. 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 n° 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

5.4.2. 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 n° 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.

5.4.3. 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 n° 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.

5.4.4. Information security management system

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

5.5. Governance

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

5.6. Planning

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

5.6.1.1. General points

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

5.6.1.2. Risk assessment

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

Requirement n° 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.

5.6.1.3. Risk treatment

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

Requirement n° 06

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

Requirement n° 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 n° 08

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

5.6.2. 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 n° 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.

5.6.3. Planning of changes

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

5.7. Media

5.7.1. Resources

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

5.7.2. Competence

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

5.7.3. Awareness

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

Requirement n° 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.

5.7.4. Communication

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

Requirement n° 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 n° 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.

5.7.5. Documented information

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

5.8. Operation

5.8.1. Operational planning and control

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

Requirement n° 13

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

5.8.2. Risk assessment

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

5.8.3. Risk treatment

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

Requirement n° 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

5.9. Performance evaluation

5.9.1. 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 n° 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.

5.9.2. Internal audit

5.9.2.1. General points

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

Requirement n° 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.

5.9.2.2. Internal audit programme

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

5.9.3. Management review

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

5.10. 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 GDPR1 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 n° 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[1], 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/laprotection-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 (version2.0, adopted on 18 June 2021).

Requirement n° 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 unauthorized 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 unauthorized 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 n° 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 8

Requirement n° 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 n° 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 n° 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 n° 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 n° 06

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

Requirement n° 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 n° 08

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

Requirement n° 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 n° 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 n° 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 n° 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 n° 13

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

Requirement n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 n° 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 GDPR1 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 n° 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[2], 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.

Requirement n° 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 unauthorized access covered by Requirement No 30. The arrangements for informing the public must take the following form:

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

- 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 policy	5.2 – Information security policy
5.2 – Functions and responsibilities related to information security	5.2 – 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
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
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
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

Measure Annex A	Applicable SecNumCloud Requirements
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
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
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

Measure Annex A	Applicable SecNumCloud Requirements
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
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 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).