HDS Accreditation framework

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

This document is the English version of HDS Accreditation framework – 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

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 v2.0

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

Détermination du temps d'audit des systèmes de management de la qualité et des systèmes de management environnemental

Reference no 8 : IAF MD11 version in force

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

The IAF requirements documents are available on the IAF website.

SUMMARY

1. INTRODUCTION

1.1. 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.

1.2. 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.

1.2.1. Definitions

1.2.1.1. 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.

1.2.1.2. 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..

1.2.1.3. 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.

1.2.1.4. 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").

1.2.1.5. 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.

1.2.1.6. 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.

2. SCOPE

2.1. 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.

2.1.1. 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.

2.1.2. Nature of the data

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

2.1.3. 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.

2.1.4. 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 1.2.1.2

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.

3. 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.*

4. 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)

5. 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.

5.1. 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.

5.2. Accreditation requirements

5.2.1. General requirements

5.2.1.1. Contractual and legal area

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

5.2.1.2. Impartiality management

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

5.2.1.3. Responsibility and financing

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

5.2.2. Structural requirements

5.2.2.1. 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.

5.2.2.2. 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.

5.2.2.3. Intervention of individual external auditors and technical experts

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

5.2.2.4. Staff records

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

5.2.2.5. Outsourcing

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

5.2.3. Information requirements

5.2.3.1. Publicly available information

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

5.2.3.2. 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..

5.2.3.3. Reference to certification and use of trademarks

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

5.2.3.4. 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..

5.2.3.5. Exchange of information with the competent authority

5.2.3.5.1. 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.

5.2.3.5.2. Rapport de retrait HDS

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.

5.2.3.5.3. 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.

5.2.3.5.4. 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.

5.2.4. Certification process requirements

5.2.4.1. Pre-certification activities

5.2.4.1.1. 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.

5.2.4.1.2. Review of the application

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

5.2.4.1.3. 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.

5.2.4.1.4. 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).

5.2.4.1.5. Multiple sampling

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

5.2.4.1.6. 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.

5.2.4.2. Audit planning

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

5.2.4.3. Initial certification

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

5.2.4.4. 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.

5.2.4.5. Certification decision

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

5.2.4.6. 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.

5.2.4.7. Appeals

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

5.2.4.8. Complaints

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

5.2.4.9. Client records

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

5.2.4.10. Management system requirements for certification bodies

5.2.4.10.1. Options

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

5.2.4.10.2. Management system requirements in accordance with ISO 9001

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

5.2.4.10.3. General management system requirements

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

5.2.5. Assessment procedures

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

6. 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.

6.1. 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

6.2. Accreditation suspension process

6.2.1. 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.

6.2.2. 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.

6.3. 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.

6.4. Transfert de certification à un nouvel organisme de certification à la suite d'un retrait

The new certification body receiving a transfer request must apply the provisions described in §**Erreur ! Source du renvoi introuvable.**. 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.

6.5. 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.

7. CONDITIONS, CRITERIA AND PROCEDURES FOR CERTIFICATION

7.1. 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 7.2

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 7.2.

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.

7.2. 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.

7.3. Subcontracting

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

Annexe 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[1]
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
2026 – 2675	22	4	26
2676 – 3450	23	4	27
3451 – 4350	24	5	29

[1] 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
4351 – 5450	25	5	30
5451 – 6800	26	5	31
6801 – 8500	27	5	32
8501 - 10700	28	5	33
10701	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.

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

HDS annual report

Name of certification Body : XXX	**Date : jj/mm/aaaa**

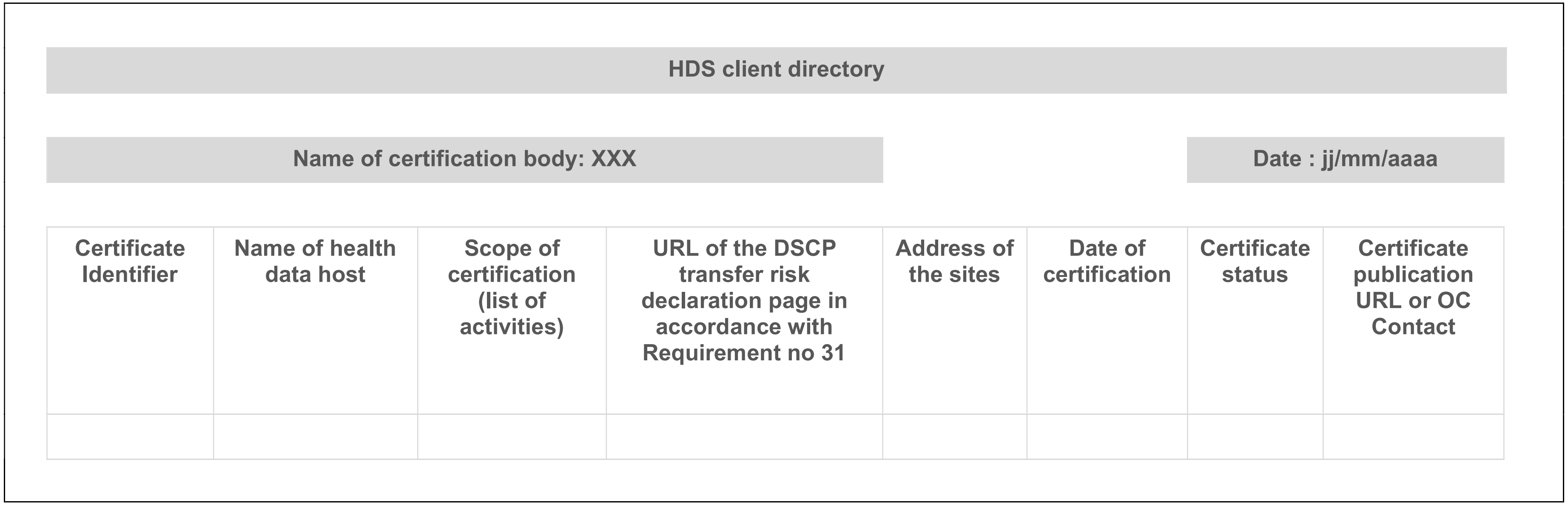
Summary of HDS certifications, audits performed and non-conformities identified

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



HDS client directory

Name of certification body: XXX

Date : jj/mm/aaaa

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