La certification pour l'hébergement de données de santé à caractère personnel (HDS)

Olivier Rouchon

DDOR-CNRS

olivier.rouchon@cnrs.fr

Le cadre juridique

Les modalités sont encadrées par l'article L.1111-8 du code de la santé publique :

- toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet ;
- l'hébergement exige une information claire et préalable de la personne concernée par les données de santé hébergées et une possibilité pour celle-ci de s'y opposer pour motif légitime.

Cet article distingue explicitement trois grandes catégories de :

- l'hébergement de données de santé sur support papier
- l'hébergement de données de santé sur support numérique dans le cadre d'un service d'archivage électronique
- l'hébergement de données de santé sur support numérique (hors cas d'un service d'archivage électronique)

L’historique

- Avant Avril 2018, l’agrément était délivré par le ministère chargé de la Santé sur la base d’un dossier remis à l’ASIP-Santé et après avis de la CNIL et du comité d’agrément des hébergeurs.
- La **nouvelle procédure de certification** pour l’hébergement de données de santé à caractère personnel sur support numérique la remplace depuis. Elle prévoit d’encadrer l’activité d’hébergement de données de santé par une **évaluation de conformité à un référentiel de certification**, délivrée par un organisme de certification accrédité par le COFRAC.
- Le décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel définit la nouvelle procédure de certification.
- Les référentiels d’accréditation et de certification ont été publiés au Journal Officiel de la République française pour l’ouverture du guichet de la procédure de certification.

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

cofrac

La certification

Deux types de certificats seront délivrés aux hébergeurs pour deux métiers d'hébergement distincts :

- un certificat « hébergeur d'infrastructure physique » ;
- un certificat « hébergeur infogéreur » ;

Si l'activité de l'hébergeur s'inscrit dans les deux types d'activité, l'hébergeur doit obtenir les deux certifications.

L’hébergeur d’infrastructure physique

1. Mise à disposition et maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
2. Mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.

L’hébergeur infogéreur

3. Mise à disposition et maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
4. Mise à disposition et maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
5. Administration et exploitation du système d'information contenant les données de santé ;
6. Sauvegardes externalisées des données de santé.

Le référentiel de certification

Le référentiel de certification s'appuie sur des normes internationales :

- La norme ISO 27001 « système de gestion de la sécurité des systèmes d'information » ;
- 4 exigences de la norme ISO 20000-1 « système de gestion de la qualité des services » ;
- 25 exigences de protection de données à caractère personnel pour lesquelles une conformité à la norme ISO 27018 confère une présomption de conformité ;

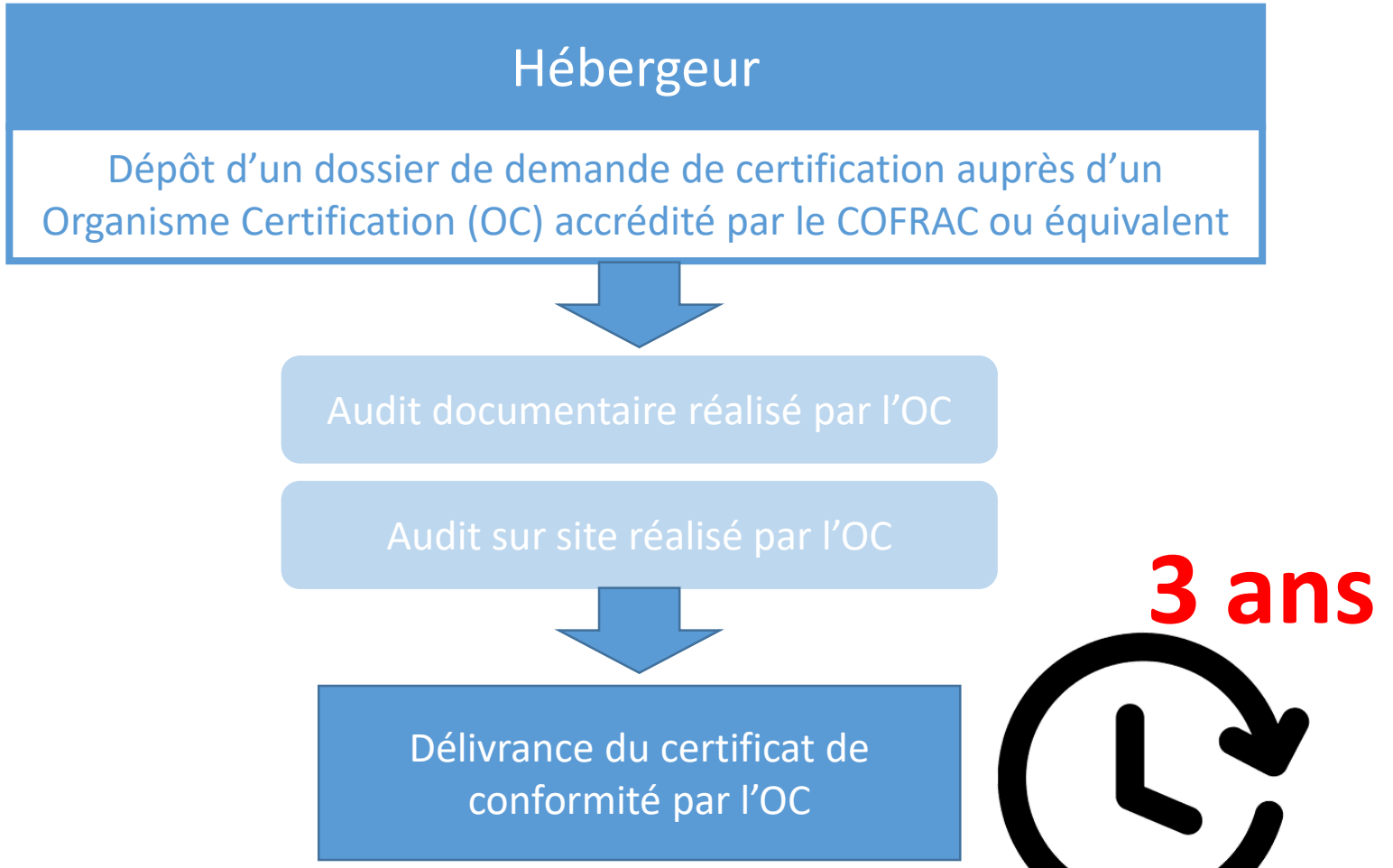
Et des compléments spécifiques à l'hébergement de données de santé :

- 11 exigences sur la protection des données de santé à caractère personnel (droit des personnes, finalité, communication, transparence, responsabilité, sécurité, etc.) ;
- 4 exigences sur la conformité à la PGSSI-S, rapports d'audit, etc.

AGENCE DU NUMÉRIQUE EN SANTÉ

La procédure de certification

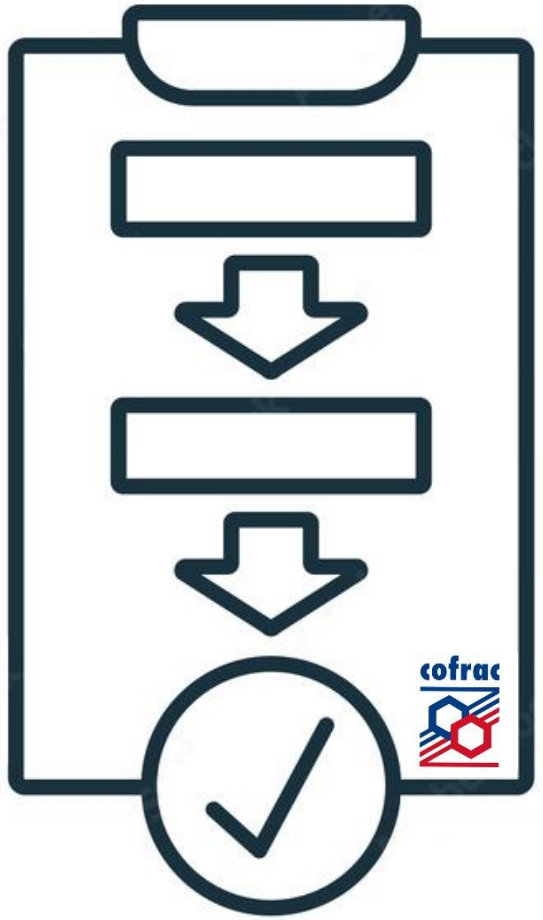
- Le certificat est délivré pour une durée de trois ans, par l'organisme certificateur, lorsqu'aucune non-conformité n'est constatée.
- Un audit de surveillance annuel est effectué par l'organisme certificateur



La procédure de certification

La procédure de certification se fonde sur le processus standard de type système de management décrit dans la norme ISO 17021 :

- L'hébergeur choisit un organisme certificateur accrédité par le COFRAC (ou équivalent au niveau européen).
- Le cas échéant, l'organisme certificateur vérifie l'équivalence des éventuelles certifications ISO 27001 ou ISO 20000-1 déjà obtenues par l'hébergeur.



La procédure de certification

Un audit en deux étapes :

- Audit documentaire : l'organisme certificateur réalise une revue documentaire du système d'information du candidat afin de déterminer la conformité documentaire du système par rapport aux exigences du référentiel de certification ;
- Audit sur site : les preuves d'audit sont recueillies dans les conditions définies dans le référentiel d'accréditation. L'hébergeur dispose de trois mois après la fin de l'audit sur site pour corriger les éventuelles non-conformités et faire auditer les corrections par l'organisme certificateur. Passé ce délai et sans action de l'hébergeur, l'audit sur site devra être recommencé.

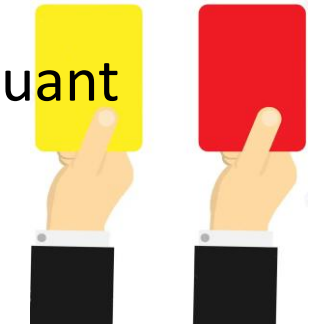
Les perspectives

Vers un nouveau référentiel de certification HDS

- Projet de référentiel porté par l'Agence numérique en santé ;
- Publication pour commentaires le 2/11/2022, jusqu'au 9/12/2022
- L'objectif de la révision est triple :
  - Améliorer la lisibilité des garanties apportées par un hébergeur certifié sur les prestations réalisées pour un client donné ;
  - Clarifier les obligations contractuelles d'un prestataire faisant appel aux services d'un hébergeur certifié ;
  - Renforcer les exigences de protection des données personnelles au regard des transferts hors UE.
- Adoption au printemps 2023 avec des premières certifications en octobre 2023 ?

Les sanctions

- Les manquements à l'Article L.1111-8 CSP sont sanctionnés par une peine allant jusqu'à 3 ans d'emprisonnement et une amende pouvant atteindre 45.000 € ou 225.000 € pour les personnes morales.
- Les traitements de données personnelles en infraction à cette réglementation peuvent aussi donner lieu à une sanction de la CNIL et notamment une injonction de cesser le traitement et /ou une amende administrative pouvant aller jusqu'à 3 millions ou à compter de l'entrée en vigueur du RGPD le 25 mai 2018 jusqu'à 20 million ou 4% du chiffre d'affaire mondial.
- Les montages contractuels et autres pratiques visant à se soustraire à l'obligation d'agrément, par exemple le fait de nommer le contrat d'hébergement « contrat de bail », peuvent conduire à mettre en jeu la responsabilité pénale de « l'hébergeur », l'hébergement de données de santé sans agrément constituant notamment un délit, puni de trois ans d'emprisonnement et de 45 000 € d'amende (articles L.1115-1 et L.1115-2 du CSP).



La bibliographie

- Article L1111-8 du code de la santé publique : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549
- Les référentiels de la procédure de certification : https://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/les-referentiels-de-la-procedure-de-certification
- Le projet de nouveau référentiel : https://esante.gouv.fr/sites/default/files/media_entity/documents/20221028-exigences-hds-1.1.pdf
- Corpus documentaire de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) : https://esante.gouv.fr/produits-services/pgssi-s

Des questions ?

Le modèle de certification Européen

Certification formelle ISO 16363:2012
(1 Centre certifié, 100+ critères)
www.iso16363.org/

Certification étendue DIN 31644
(4 Centres certifiés, 34 critères)
www.langzeitarchivierung.de

Certification CoreTrustSeal
(170+ centres, 16 critères)
www.CoreTrustSeal.org

Centres de données de confiance - Trustworthy Data Repositories