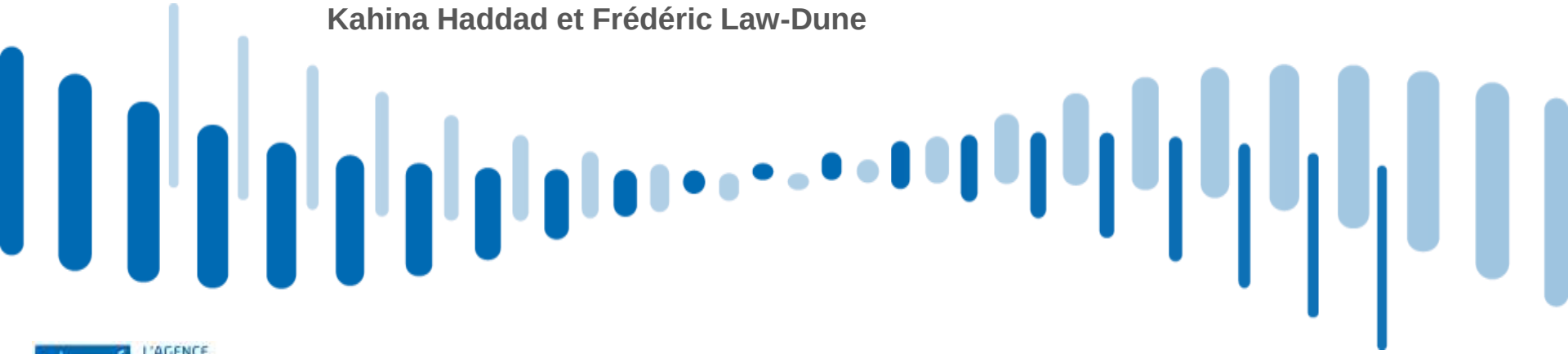
Journée Nationale des Industriels

21 décembre 2017

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Atelier certification des hébergeurs de données de santé

Kahina Haddad et Frédéric Law-Dune



Cadre juridique et calendrier

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

L'encadrement de l'hébergement de données de santé depuis l'ordonnance du 12 janvier 2017

L'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel modifie largement l'article L.1111-8 du code de la santé publique en distinguant dorénavant **trois types de décisions préalables pour l'hébergement de données de santé :**

1. **Hébergement de données de santé sur support informatique :**
   Certificat de conformité délivré par un organisme de certification accrédité par le COFRAC (ou équivalent)

2. **Hébergement de données de santé dans le cadre d'un service d'archivage électronique :**
   Agrément délivré par le ministre chargé de la culture

3. **Hébergement de données de santé sur support papier :**
   Agrément délivré par le ministre chargé de la culture

La date d'entrée en vigueur de l'ordonnance sera définie par décret(s) en Conseil d'Etat

Le champ d’application de l’hébergement de données de santé

L’activité d’hébergement de données de santé à caractère personnel consiste à héberger les données de santé à caractère personnel recueillies à l’occasion d’activités de prévention, de diagnostic, de soins ou de suivi social et médico-social :

- 1° pour le compte de personnes physiques ou morales, responsables de traitement au sens de la loi n°78-17 du 6 janvier 1978, à l’origine de la production ou du recueil de ces données ;

- 2° pour le compte du patient lui-même.

Les activités d’hébergement de données de santé à caractère personnel qui relèvent de la procédure de certification sont définies par le décret relatif à l’hébergement de données de santé - qui sera prochainement publié – et par le référentiel de certification.

Calendrier et phase transitoire : de l'agrément à la certification

Décret HDS publié au JOFR

Dernier jour du mois de publication du texte : fermeture guichet agrément HDS

Entrée en application de la certification: premier jour du mois suivant la publication du texte

T0 | +1 | +2 | +3 | +4 | +5 | +6 | +7 | +8 | +9 | +10 | +11 | +12

Dossiers reçus avant la fermeture du guichet HDS

Les dossiers de demande d'agrément reçus avec la fermeture du guichet agrément sont traités selon la procédure d'agrément actuellement en vigueur

Agrément qui arrive à échéance dans l'année suivant l'entrée en application de la certification

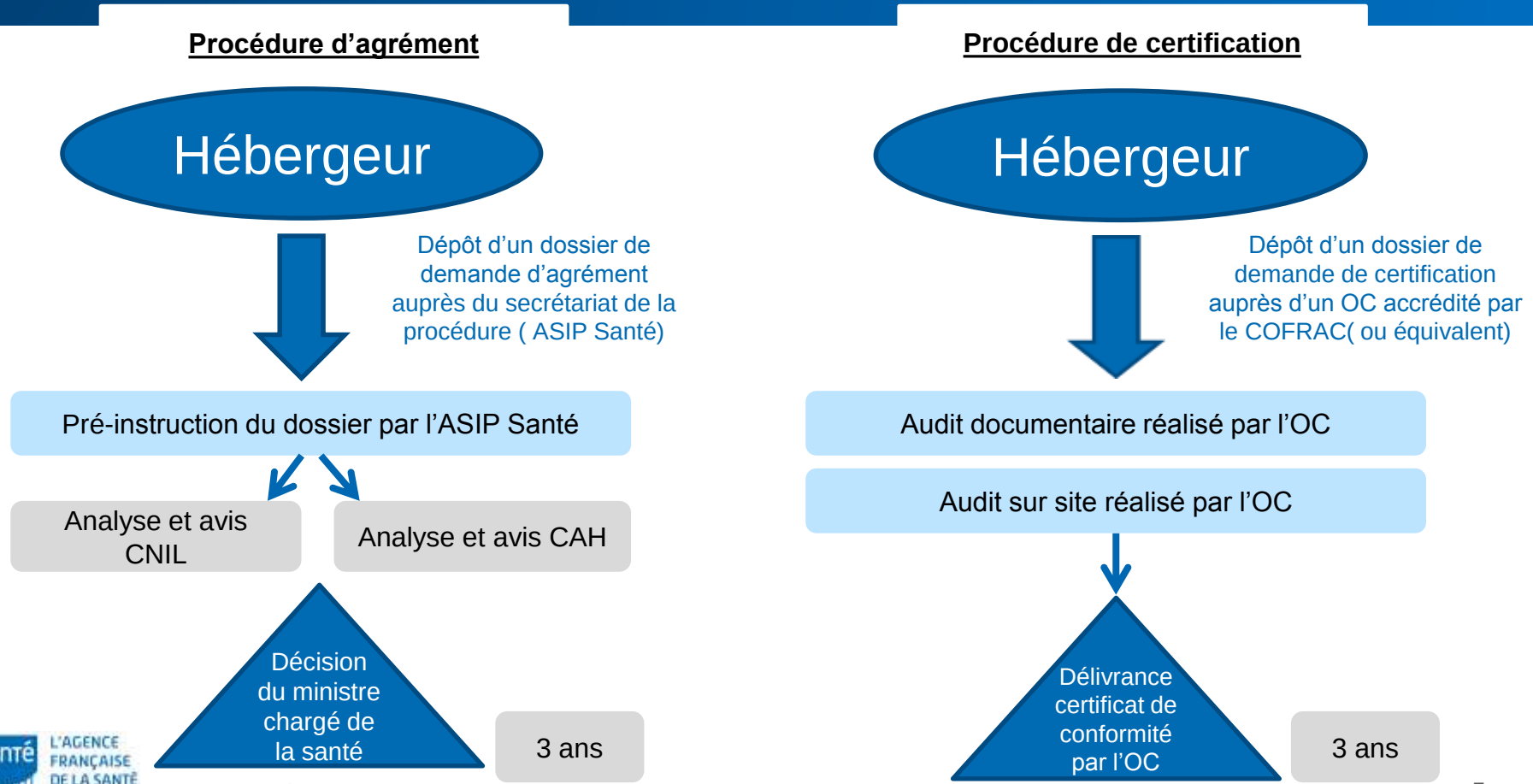
Exemple : T0+2
Fin de l'agrément

Exemple : T0+8

La décision d'agrément est encore valide 6 mois de plus

L'hébergeur doit être certifié

Vue d'ensemble des processus d'agrément et de certification



Les étapes du processus d’accréditation : de la publication des textes à la certification des hébergeurs de données de santé

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Etapes pour la mise en place d'une certification sous accréditation

1
- **Définition des règles de certification par prescripteur (1 à 3 ans)**
  - Référentiel de certification
  - Consultation des parties intéressées
  - Modalités de transition éventuelles

2
- **Information des intéressés par prescripteur**
  - Publication de tous les textes applicables (arrêtés d'application et guides de lecture inclus)
  - Des certifiés et certificateurs

3
- **Mise en conformité (délai variable selon impacts)**
  - Des certifiés
  - Des certificateurs

4
- **Accréditation des OC par le Cofrac**
  - Développement du schéma d'accréditation (9 à 12 mois à partir d'un référentiel de certification avancé)
  - Pour le schéma HDS, le développement a été initié dès la fin de l'étape 1
  - Processus d'accréditation à partir de la publication des textes (selon état des OC candidats, au moins 1 an après recevabilité documentaire)

De la publication des textes à la certification des hébergeurs de données de santé

- PUBLICATION DES TEXTES REGLEMENTAIRES ET DES REFERENTIELS DE L'ASIP SANTE
- OUVERTURE DU SCHEMA D'ACCREDITATION par le COFRAC
- ECEPTION DES DOSSIERS DE CANDIDATURE DES ORGANISMES DE CERTIFICATION (OC)
- RECEVABILITE ADMINISTRATIVE ET SIGNATURE DU CONTRAT
- RECEVABILITE TECHNIQUE
  (délai variable entre 1 et 6 mois après la signature du contrat)
- CONFIRMATION DE LA RECEVABILITE TECHNIQUE
- RGANISATION DE L'EVALUATION SIEGE + OBSERVATION D'AUDIT
  (Dès lors que les OC ont démarré les certifications des HDS)

En parallèle

Mise en conformité des OC et des Hébergeurs avec les textes et les référentiels avant de pouvoir déposer une demande d'accréditation (OC) ou une demande de certification (HDS)

Dès cette étape validée

Les OC sont autorisés à délivrer des certificats non accrédités pendant neuf (9) mois et devront obtenir l'accréditation pendant cette période

Calendrier d'ouverture de procédure de certification

Décret HDS publié au JOFR

Dernier jour du mois de publication du texte : fermeture guichet agrément HDS

Entrée en application de la certification: premier jour du mois suivant la publication du texte

T0 | +1 | +2 | +3 | +4 | +5 | +6 | +7 | +8 | +9 | +10 | +11 | +12

Ouverture de l'accréditation HDS pour les **OC**
Possibilité pour les OC de déposer un dossier auprès du COFRAC

Ouverture de la certification HDS pour les hébergeurs (par un OC)
Possibilité pour un hébergeur de déposer une demande de certification auprès d'un OC

Périmètre de la certification et procédure de certification

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Deux niveaux de certificats pour deux métiers d'hébergement distincts

Hébergeur d'infrastructure physique

1. Mise à disposition ou maintien en condition opérationnelle de locaux permettant d'héberger l'infrastructure matérielle du système d'information de santé
2. Mise à disposition ou maintien en condition opérationnelle de l'infrastructure matérielle du système d'information de santé

Hébergeur infogéreur

3. Mise à disposition ou maintien en condition opérationnelle de la plateforme logicielle (système d'exploitation, middleware, base de données, etc.) du système d'information de santé
4. Mise à disposition ou maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information de santé
5. Infogérance d'exploitation du système d'information de santé
6. Sauvegardes externalisées des données de santé

Le choix du périmètre de la certification

Un hébergeur souhaitant obtenir une certification pour l'hébergement de données de santé doit identifier les activités concernées par sa demande

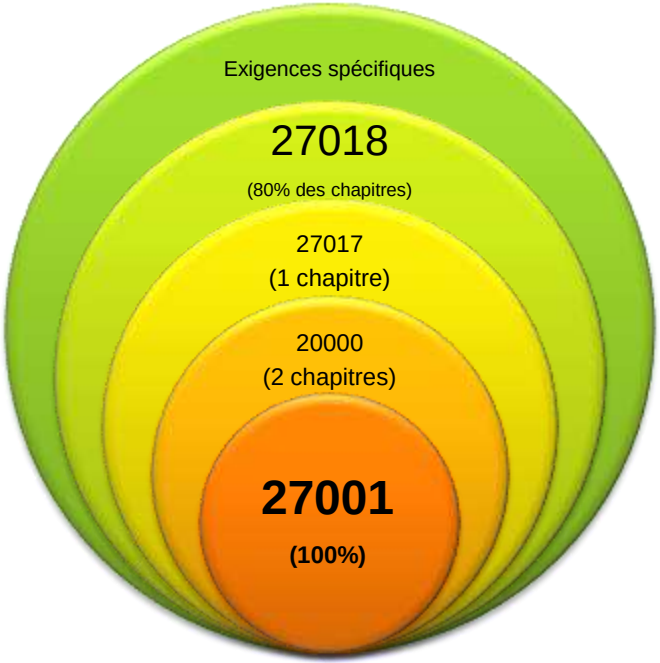
- Lorsque le périmètre d'activités comprend exclusivement une ou plusieurs activités parmi les **activités numérotées de 1 à 2**, il est évalué pour la conformité aux exigences s'appliquant aux hébergeurs d'infrastructure physique. La certification obtenue est dénommée certification **« hébergeur d'infrastructure physique ».**

- Lorsque le périmètre d'activités comprend exclusivement une ou plusieurs activités parmi les **activités numérotées de 3 à 6**, il est évalué pour la conformité aux exigences s'appliquant aux hébergeurs infogéreurs. La certification obtenue est dénommée certification « **hébergeur infogéreur** ».

- Lorsque le périmètre comprend **au moins une activité de chacun de ces périmètres**, il est évalué pour la conformité à toutes les exigences et obtient les **deux certifications**.

Définition de la certification HDS en 3 mots

Certification HDS = Certification 27001 complétée



La procédure de certification et son référentiel

- **La procédure de certification se fonde sur le processus standard de type système de management décrit dans la norme ISO 17021 et précisé dans la norme ISO 27006 :**
  - **l'hébergeur choisit un organisme certificateur accrédité par le COFRAC (ou équivalent au niveau européen) ;**
  - **l'organisme certificateur vérifie l'équivalence des éventuelles certifications ISO 27001 ou ISO 20000 déjà obtenues par l'hébergeur ;**
  - **un audit en deux étapes conformes aux normes en vigueur est alors effectué :**

Etape 1 — **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.

Etape 2 — **Audit sur site**

Les preuves d'audit sont recueillies dans les conditions définies dans le référentiel d'accréditation basé sur les normes l'ISO 17021 et ISO 27006.
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.

La procédure de certification et son référentiel

- **Le référentiel de certification est composé de**
  - la norme ISO 27001 « système de gestion de la sécurité des systèmes d'information »,
  - d'exigences de la norme ISO 20000 « système de gestion de la qualité des services»,
  - d'exigences de la norme ISO 27018 « protection des données à caractère personnel »
  - d'une exigence de la norme ISO 27017 « Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage »
  - et d'exigences spécifiques à l'hébergement de données de santé.

Le détail des exigences pour les certifications d'hébergeur d'infrastructure physique et d'hébergeur infogéreur seront prochainement mis à disposition sur le site de l'ASIP Santé, esante.gouv.fr

- **Une dimension internationale**
  - La certification HDS pourra être délivrée par tout organisme certificateur accrédité par un organisme d'accréditation européen signataire des accords de reconnaissance EA/IAF.

La procédure de certification et son référentiel

- **Pour obtenir une certification HDS, un candidat doit :**

Être certifié ISO 27001

Être évalué sur sa conformité aux exigences issues des normes (20000, 27017, 27018) et des exigences spécifiques

- **Validité du certificat**

3 ans — **Le certificat est délivré pour une durée de trois ans, par l'organisme certificateur**

1 an — **Un audit de surveillance annuel est effectué par l'organisme certificateur**

Questions

Questions fréquentes

1. Hébergement de données de santé …

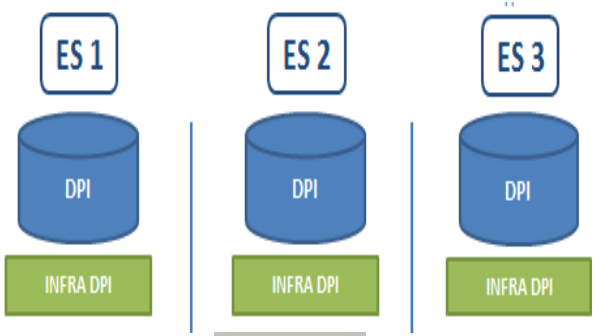
… et RGPD

- Qualification de l'hébergeur ? Contenu minimal du contrat HDS ?
- Consentement au traitement ou information relative au traitement ≠ information + droit d'opposition à l'hébergement externalisé

… et PGSSI-S

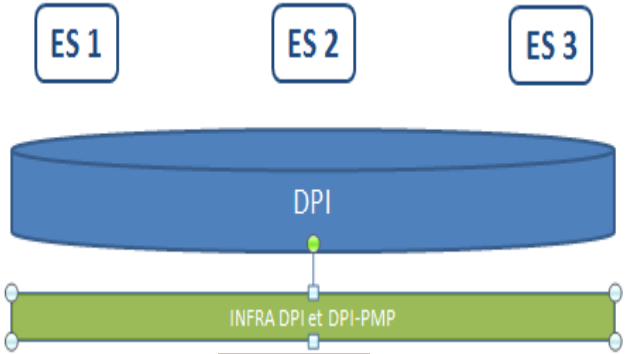
Questions fréquentes

2. Hébergement de données de santé et GHT



Cas 1

Cas 2



Cas 3

Autres Questions ?

- **Echanges sur la question de « l'externalisation locale et sur mesure »**
- **Echanges sur l'étendue d'un certification de conformité délivrer à la maison mère**
- **Autres ?**

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'ASIP Santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/asip-sante