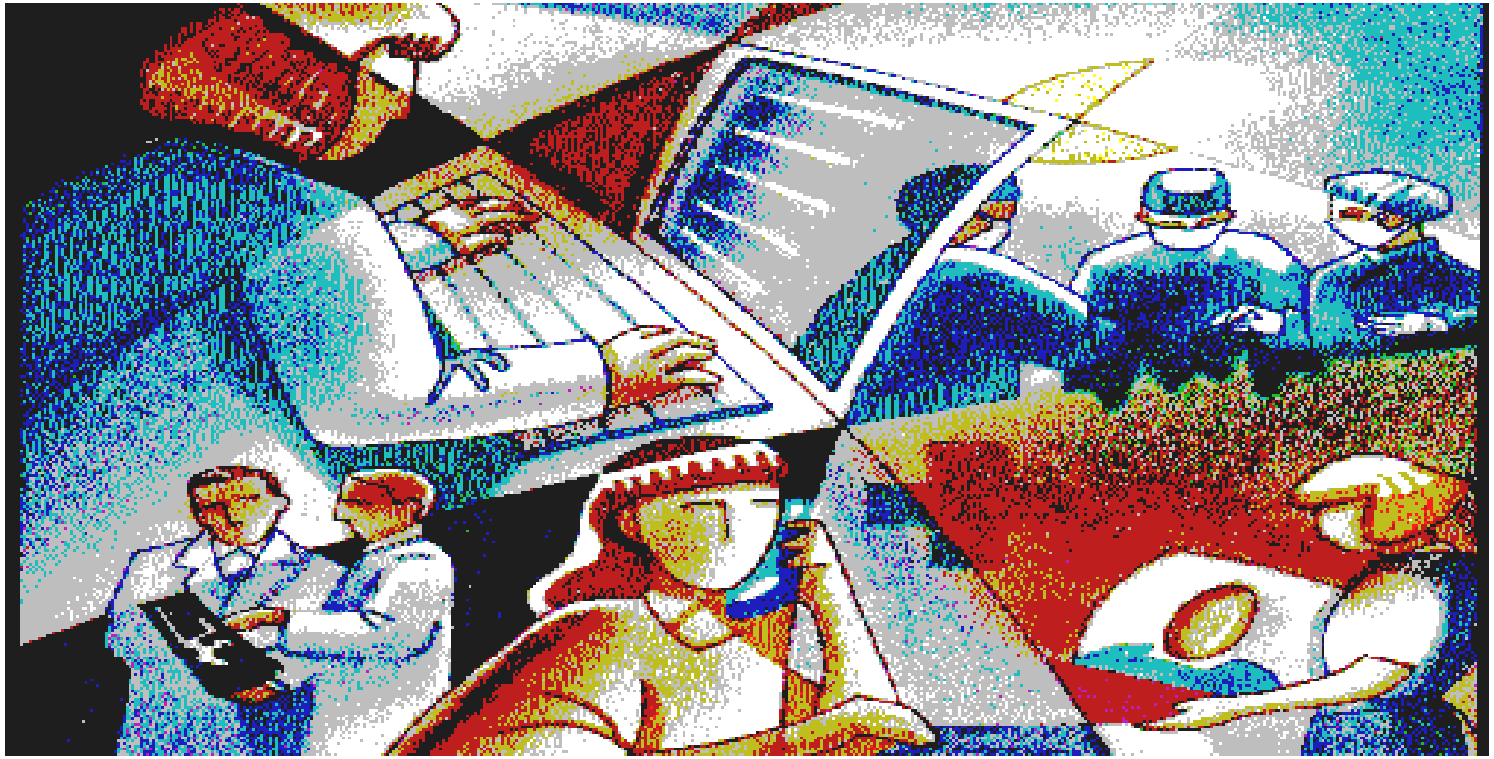


L’hébergement de données de Santé à caractère personnel

pci/rph
Le lien entre systèmes & applicatifs

L'hébergement de données de santé à caractère personnel

- ✓ Principe de droit à l'information et à la confidentialité
- ✓ Evolution des SIH classiques vers un mode de partage
- ✓ L'hébergeur doit être agrée pour son activité (ART L.1111.8 du CSP)
- ✓ Condition de délivrance fixées par décret en conseil d'état du 4 janvier 2006
  - Codifié aux ART R.1111-9 à R.1111-14 du CSP
- ✓ La CNIL se prononce sur la protection des personnes
  - ➢ Dépôt de dossier auprès de l'ASIP (Agence des Systèmes d'Information Partagés de Santé).

Dépôt de dossier : le référentiel

- ✓ Fixé par l' ART L.1111-8 du CSP (voir projet de décret modifiant l'article)
- ✓ Inséré par la loi n° 2002-303 du 4 mars 2002 (dite loi Kouchner)
- ✓ Condition de délivrance fixées par décret en conseil d'état du 4 janvier 2006
  - Codifié aux ART R.1111-9 à R.1111-14 du CSP

➢ Formulaires disponibles sur le site de l'ASIP.

Formulaires

P1) Formulaire de présentation détaillée du candidat :

P2) Formulaire de présentation détaillée d'un sous-traitant :

P3) Formulaire de description des clauses d'un modèle de contrat :

P4) Formulaire de présentation du service d'hébergement :

P5) Formulaire de présentation des résultats de l'analyse des risques :

P6) Formulaire de description des dispositions de sécurité :

P1 : Formulaire de présentation détaillée du candidat

Ce document a pour objet de structurer le recueil des informations demandées au candidat au titre des alinéas 1, 2, 3, 7 et 8 de l'article R. 1111-12 du décret n° 2006-6 du 4 janvier 2006.
Les pièces administratives relatives au candidat seront fournies en annexe.
Il précisera l'identification du responsable du service d'hébergement.
Les rôles et fonction du médecin hébergeur qui doit être enregistré à l'ordre des médecins, son contrat de travail.
Les catégories de personnes ayant accès aux données selon l'article R1111-12 2° deuxième Partie.
Les opérateurs chargés de mettre en œuvre le service selon l'article R1111-12 2° première partie.
Les sous-traitants éventuels selon l'Art. R. 1111-12 7°.
Les renseignements d'ordre financier du candidat selon Art. R. 1111-12 8°

P2 : Formulaire de présentation détaillée Sous-Traitant

Ce document a pour objet de structurer le recueil des informations demandées au candidat au titre des alinéas 1, 2, 3, 7 et 8 de l'article R. 1111-12 du décret n° 2006-6 du 4 janvier 2006.

L'identification des sous-traitants sera conforma à l'Art. R. 1111-12 1°.

Les pièces administratives relatives au candidat seront fournies en annexe.

La localisation des prestations selon Art. R.1111-12 3°

Les catégories des personnes ayant accès aux données selon Art. 1111-12 2° deuxième partie.

Les opérateurs chargés de mettre en Œuvre le service selon Art. R.1111-12 2° première partie.

Les renseignements relatifs à la situation financière selon Art. R. 1111-12 8°

Les comptes prévisionnels de l'activité selon Art. R. 1111-12 8°

P3 : Formulaire de description des clauses d'un modèle de contrat

Ce formulaire correspond au recueil des informations exigées par les dispositions des articles R. 1111-12 alinéas 5° et R. 1111-13 du décret n°2006-6 du 4 janvier 2006.

Le modèle de contrat devant être joint à la demande d'agrément contient obligatoirement au moins les clauses suivantes telles quelles sont exigées par l'article R. 1111-13.

Pour chacune des clauses demandées, selon les articles en référence, nous préciserons les pages, paragraphe ou article concerné dudit contrat.

P4 : Formulaire de présentation du Service d'Hébergement

Informations demandées selon les principes généraux relatifs au décret N° 2006-6 du 4 janvier 2006 concernant l'Hébergement de données de santé à caractère personnel et selon les dispositions réglementaires.
A prendre en considération :
- la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.
- la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.
- le décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques.
- le décret n° 97-34 du 15 janvier 1997 modifié relatif à la déconcentration des décisions administratives individuelles,
- le décret n° 97-1185 du 19 décembre 1997 modifié pris pour l'application à la ministre de l'emploi et de la solidarité du 1° de l'article 2 du décret du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles.

P5 : Formulaire de présentation des résultats de l'analyse des risques.

Ce document a pour objet de structurer le recueil des résultats de l'analyse des risques relatifs à la sécurité du système d'information constitutif du service proposé.
Les informations recueillies dans ce formulaire concourent à la présentation des dispositions prises pour assurer la sécurité des données comme demandée à l'article R. 1111.12 6°.

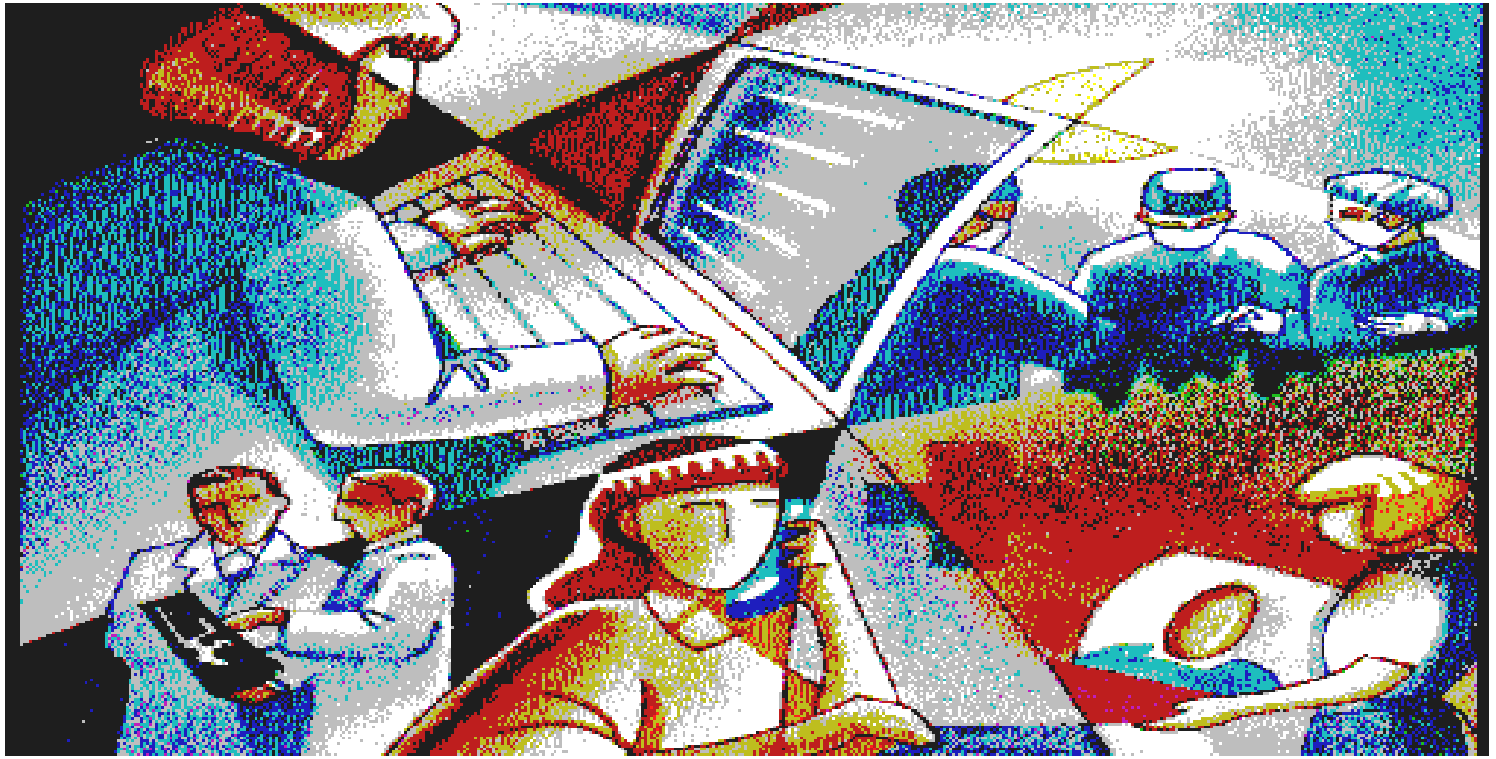
Nous avons opté pour le choix de la méthode **EBIOS** car elle est reconnue par la DCSSI, le développement est français et les droits sont libres.

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'identifier les risques d'un SI et de proposer une politique de sécurité adaptée aux besoins de l'entreprise (ou d'une administration).
Elle a été créée par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), du Ministère de la Défense (France). Elle est destinée avant tout aux administrations françaises et aux entreprises.

P6 : Formulaire de description des dispositions de sécurité.

Ce document a pour objet de structurer le recueil des informations demandées au candidat au titre du décret n° 2006-6 du 4 janvier 2006 à l'article R. 1111-4.
Notre document présentera l'organisation et la gestion de la sécurité (PSSI).
Notre accompagnement à la rédaction de la politique de sécurité sur le périmètre de l 'hébergement ou pour une politique technique.
Notre formulaire des dispositions de sécurité abordera les points suivants :

- L'organisation
- Le respect du droit des personnes
- Les ressources Humaines
- Contrôle d'accès
- Télécommunications
- Traçabilité
- Gestion des incidents
- La sauvegarde et l'archivage des données
- L'archive
- La continuité de service
- La gestion des évolutions
- La conformité



HDS
&
RGPD

pci/rph
Le lien entre systèmes & applicatifs

Rappels

- Article L111-8 du code de la santé publique inséré par la loi n° 2002-303 du 4 mars 2002, dite loi « Kouchner »

La protection des personnes physiques ayant mis à disposition d'un organisme ses données de santé à caractère personnel.

- L'agrément est délivré par le ministre chargé de la santé, après avis motivé d'un comité d'agrément (ASIP) et de la CNIL pour une durée de 3 ans.

Nouvelle procédure

- Nouvelle procédure de certification

  Un décret d'application devra valider ce modèle, modèle validé par un organisme de type COFRAC

  - En principe une mise en œuvre de cette nouvelle procédure « Janvier 2018 »

Nouvelle procédure

- **La certification se fonde sur des normes internationales**

  - ISO 27001 "système de gestion de la sécurité des systèmes d'information",
  - ISO 20000 "système de gestion de la qualité des services »
  - ISO 27017 "code de pratique pour les contrôles de sécurité de l'information pour les services du nuage »
  - ISO 27018 "protection des données à caractère personnel".

  ✓ Un processus décrit dans la norme ISO/CEI 17021.

RGPD

- L’union Européenne a adopté le nouveau règlement sur la protection des données.

RGPD : Règlement Général sur la Protection des Données

Applicable à partir du 25 mai 2018 en complément et mise à jour de la loi informatique et libertés du 6 janvier 1978

- Assurer une équivalence dans le traitement des données à caractère personnel dans tous les états membres
- La libre circulation des données à caractère personnel au sein de l’Union ne sera ni limitée, ni interdite pour des motifs liées à la protection des personnes physiques.
- Le RGPD ne couvre pas le traitement des données à caractère personnel concernant les personnes morales
- Réclamation possible auprès d’une autorité unique

RGPD

- L'union Européenne a adopté le nouveau règlement sur la protection des données.

RGPD : Règlement Général sur la Protection des Données

- Intégration de la **pseudonymisation** par les Entreprises pour la protection des données à caractère personnel dans la conception des infrastructures logiques et physique.

Pseudonymisation :
Traitement de données à caractère personnel de sorte que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumise à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

- Incidents graves de sécurité des systèmes d'information

  Décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information (publication JORF n°0214 du 14 septembre 2016 texte n°15)

  - Les dispositions du présent décret entrent en vigueur le 1 er octobre 2017

- Sont considérés comme incidents graves de sécurité des Systèmes d'information

D'ordre général sur la sécurité des soins

- ✓ Conséquence sur la confidentialité
- ✓ Sur l'intégrité des données de santé
- ✓ Sur le dysfonctionnement d'un établissement de soins suite à un incident

L’entrée en vigueur du Règlement Général sur la Protection des Données (RGPD)

- ✓ L’obligation d’établir un dossier de conformité, permettant à tout moment de démontrer la conformité du traitement aux principes énoncés dans la le RGPD et aux mesures de sécurité standard

- ✓ Une augmentation colossale des sanctions : la sanctions administrative de 3 M€ d’amende depuis l’automne 2016 va passer à 20 M€ d’amende ou 4 % du CA Mondial.