Recueil des textes de lois, référentiels et guides applicables aux SI de Santé

Note aux nouveaux venus dans la fonction

Le référentiel de la PGSSI-S fournit une PSSI dotée d'exigences techniques directement applicables.
https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi-s_pssi_guide_documents_supports.zip

Elle constitue un référentiel conforme aux loi applicables en 2015 en particulier les PSSI-E et PSSI MCAS et couvre les différents référentiels parus en 2016-2022 (Instruction 309, mesure prioritaires, Hopen, PSSI-MCAS, directive NISv1). Elle doit cependant être revue pour prendre en compte le RGPD et le besoin d'hébergement intra-européen. Elle ne prend également pas en compte la classification des données de l'ISO27001.
Il s'agit d'une bonne base si l'on ne souhaite pas aller sur du 27001 directement.

Lois/Instructions/Circulaires

- La loi N° 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- **L'Article L1111-8 - Code de la santé publique relatif à l'hébergement de données de santé (hébergement HDS)**
- Article 9 du code civil.
- La législation relative à la fraude informatique (article 323-1 à 323-7 du Code Pénal).
- La loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.
- Les dispositions du Code de la propriété intellectuelle relatives à la propriété littéraire et artistique, aux marques, dessins ou modèles.
- La loi du 4 août 1994 relative à l'emploi de la langue française.
- Le Code des postes et des communications électroniques.
- La législation applicable en matière de cryptologie, notamment l'article 28 de la loi du 29 décembre 1990 sur la réglementation des télécommunications dans sa rédaction issue de l'article 17 de la loi du 26 juillet 1996 et par ses décrets d'application du 24 février 1998, 23 mars 1998 et 17 mars 1999.
- La directive 96/9CE du 11 mars 1996 concernant la protection juridique des bases de données.
- La loi N° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (valeur probante des support papiers et signature electronique).
- La loi N° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (handicap).
- La loi N° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

- Article 227-23 du Code Pénal, qui criminalise le fait de fixer, d'enregistrer ou de transmettre, en vue de sa diffusion, l'image ou la représentation d'un mineur qui présente un caractère pornographique.
- ~~Le décret N° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques.~~ (modifié par Décret n° 2016-994 du 20 juillet 2016)
- ~~Le décret N° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel.~~ (modifié par Décret n° 2016-994 du 20 juillet 2016)
- ~~Le décret N° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique. (modifié par Décret n° 2016-994 du 20 juillet 2016)~~
- La loi N° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, dite loi HADOPI (Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet)
- **Le Référentiel Général de Sécurité est pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.**
- **Arrêté du 1er octobre 2015 portant approbation de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales**
- **Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.**
- **Le décret N° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information.**
- INSTRUCTION N°SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en oeuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») dans les établissements et services concernés
- **La directive NIS (Network and Information System Security) pour assurer un niveau de sécurité élevé en commun pour les réseaux et les systèmes d'information de l'Union européenne adoptée le 6 juillet 2016, publiée le 25 mai 2018 avec les règles de sécurité et les délais au 14 septembre 2018.**
- **circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État (Directive CLOUD au centre) (Hébergement en Europe)**
- **Arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé (authentification par carte CPS pour accès aux données de santé)**
- **circulaire n°6404/SG du 31 mai 2025 Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre») (SecNumCloud)**
- INSTRUCTION N° SHFDS/FSSI/2023/15 du 30 janvier 2023 relative à l'obligation de réaliser des exercices de crise cyber dans les établissements de santé et à leur financement
- INSTRUCTION N° DNS/2025/12 du 22 janvier 2025 relative à l'obligation de mettre en œuvre des actions urgentes ou prioritaires au service de la sécurité des systèmes d'information dans les établissements sanitaires

Normes :

- ISO 27001 «Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences» ;
- ISO 27002 «Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information» ;

- ISO 27003 «Techniques de sécurité —Systèmes de management de la sécurité de l'information — Lignes directrices» ;
- ISO 27005 « Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information »
- NF Z42-013 « Archivage électronique - Recommandations et exigences » octobre 2020
- NF Z42-026 « Définitions et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations »

Autres :

- Agence nationale de sécurité des systèmes d'information (ANSSI) : Guides des bonnes pratiques ;
- Introduction à la sécurité des systèmes d'information DGOS novembre 2013 ;
- Guide pratique, règles pour les dispositifs connectés d'un système d'information de santé (PGSSI-S) novembre 2013 ;
- Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaires et médico-social PGSSI-S, février 2015, ASIP Santé ;
- Guide des bonnes pratiques de l'informatique (12 règles essentielles pour sécuriser vos équipements numériques) CGPME - ANSSI mars 2015 ;
- Guide d'hygiène informatique (renforcer la sécurité de son système d'information en 42 mesures) ANSSI janvier 2017 ; https://cyber.gouv.fr/publications/guide-dhygiene-informatique ;
- Guide « Règles de sauvegarde des Systèmes d'Information de Santé (SIS) ». http://www.esante.gouv.fr/pgssi-s/espace-publication ;
- Guide « Plan de Continuité Informatique » http://www.esante.gouv.fr/pgssi-s/espace-publication ;
-Guide « Règles pour les interventions à distance sur les Systèmes d'Information de Santé (SIS) » http://www.esante.gouv.fr/pgssi-s/espace-publication ;
- Guide Pratique spécifique pour la mise en place d'un réseau WIFI de l'ASIP Santé http://esante.gouv.fr/pgssi-s/espace-publication ;
- Guide pratique « spécifique à la destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé (SIS) » http://www.esante.gouv.fr/pgssi-s/espace-publication ;

Les référentiels de sécurité :

2015 / PSSI MCAS : https://www.legifrance.gouv.fr/download/pdf?id=GoL9SuzmFwi9NS5254-oLTebC1i87nJfaqdPaNKsonw=
2015 / ***PGSSI-S*** : https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi-s_pssi_guide_documents_supports.zip
2016 / Instruction 309 : https://www.legifrance.gouv.fr/download/pdf/circ?id=41533
2018 / Directive NISv1 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037444012
2022 / Mesures Prioritaires 2022 : https://www.esante-occitanie.fr/app/uploads/2023/02/cybersecurite_referentiel_des_mesures_prioritaires.pdf

L'archivage externalisé des données de santé

(source : https://francearchives.gouv.fr/fr/article/239089579, modifiée)

Le dépôt d'archives publiques courantes et intermédiaires, sur support papier ou numérique, auprès de personnes physiques ou morales agréées à cet effet, est encadré par les textes suivants :
Code du patrimoine : articles L212-4 et R212-19 à R212-31 ;

- Arrêté ministériel du 4 décembre 2009 précisant les normes relatives aux prestations en archivage et gestion externalisée.

En plus des références citées ci-dessus, les textes suivants s'appliquent au cas particulier des données de santé à caractère personnel :

- Code de la santé publique, articles L1111-8, R1111-9 à R1111-15-1 et R1111-16 (relatifs à l'hébergement des données de santé à caractère personnel par des personnes physiques ou morales agréés à cet effet).
- Ordonnance n°2017-27 du 12 janvier 2017 relative à l'hébergement des données de santé à caractère personnel venant modifier l'article L1111-8 du Code de la santé publique et l'article L212-4 du Code du patrimoine.
- Le règlement (UE) 2016/679, dit RGPD
- La circulaire n° 6282-SG du 5 juillet 2021, dite cloud au centre

Il convient d'indiquer au préalable que, tant pour le papier que pour l'électronique, la nature privée ou publique des archives n'entre pas en ligne de compte. Cela signifie que les prescriptions évoquées ci-dessous sont applicables pour les données de santé à caractère personnel issues tant par exemple d'un établissement public hospitalier que d'une clinique privée.

Pour ce qui est du **papier**, le Code de la santé considère que l'activité d'hébergement se confond avec celle de conservation au sens défini par le Code du patrimoine et prévoit par conséquent que ces données sont confiées **uniquement** à une personne physique ou morale bénéficiant d'un **agrément** accordé au titre du Code du patrimoine (Code de la santé publique, article R.1111-16).

Pour ce qui est du **numérique**, l'article L1111-8 du code de la santé publique prévoit que l'externalisation de la conservation de données de santé à caractère personnel sur support électronique dans le cadre d'un **service d'archivage électronique** ne peut se faire qu'auprès d'une personne détentrice d'un **agrément** délivré au titre du code du patrimoine. Puisque l'activité de conservation englobe celle d'hébergement, l'agrément pour le tiers-archivage dispense donc de la certification du ministère de la Santé pour l'hébergement des données de santé (dite certification HDS) . En revanche, la certification du ministère de la santé ne dispense de l'agrément délivré au titre du code du patrimoine que si l'activité est limitée au seul hébergement*.

* Hébergement : comprend l'hébergement physique mais également le maintien en condition opérationnelle des infrastructures d'une part et des outils logiciels d'autre part mais ne comprend pas l'administration fonctionnelle d'un système d'archivage électronique et/ou la mise en œuvre des procédures archivistiques.