



**FAQ HDS &
CLOUD SANTÉ[®]
HYBRIDE AWS**

**FAQ HEALTH
DATA HOSTING &
HEALTH CLOUD[®]
HYBRID AWS**



PROTECT **PATIENTS**
& **ENABLE** HEALTH

TABLE OF CONTENTS

1- QUI EST CLOUD SANTÉ® ? - WHAT IS EURIS HEALTH CLOUD ?	P.5
2- QUI EST AMAZON WEB SERVICES (AWS) ? - WHAT IS AMAZON WEB SERVICES (AWS) ?	P.5
3- QU'EST CE QUE L'OFFRE CLOUD SANTÉ® HYBRIDE ? - WHAT IS HYBRID HEALTH CLOUD ABOUT ?	P.6
4- POURQUOI CLOUD SANTÉ® HYBRIDE - AWS? - WHY HEALTH CLOUD® HYBRID AWS ?	P.7
5- PUIS-JE HÉBERGER DES DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL (DSCP) DIRECTEMENT CHEZ AWS ? - CAN I HOST PERSONAL HEALTH DATA DIRECTLY ON AWS CLOUD ?	P.8
6- QU'EST CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ? - WHAT IS CONSIDERED AS PERSONAL DATA ?	P.8
7- QU'EST CE QUE LA DONNÉE DE SANTÉ À CARACTÈRE PERSONNEL (DSCP)? - WHAT IS CONSIDERED AS PERSONAL HEALTH DATA ?	P.8
8- QUI EST CONCERNÉ ET DOIT RECOURIR À UN HÉBERGEMENT DE DONNÉES DE SANTÉ (HDS) ? - WHO IS AFFECTED AND MUST DEPLOY A SPECIFIC HEALTH DATA HOSTING SOLUTION? (HDS IN FRANCE)	P.9
9- QU'EST CE QU'UN TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL (DSCP)? - WHAT DO WE MEAN BY PROCESSING PERSONAL DATA ?	P.9
10- QUI EST LE «RESPONSABLE DE TRAITEMENT» ? - WHO IS THE DATA CONTROLLER ?	P.10
11- L'ÉDITEUR DE LOGICIEL EST-IL «RESPONSABLE DE TRAITEMENT» ? - IS THE SOFTWARE PUBLISHER THE « DATA CONTROLLER » ?	P.10
12- QUEL EST LE RÔLE DE L'HÉBERGEUR DE DONNÉES DE SANTÉ ? - WHAT IS THE ROLE OF THE HEALTH DATA HOSTING PROVIDER ?	P.11
13- QUELLES SONT LES ACTIVITÉS DE LA CERTIFICATION HDS ? - WHAT ARE THE ACTIVITIES COVERED BY THE HDS CERTIFICATION ?	P.12
14- QUI CONSTRUIT UN CADRE CONTRACTUEL HDS GLOBAL DÉDIÉ AUX PROJETS ET AUX CONTRAINTES CLIENTS ? - WHO BUILDS A GLOBAL "HDS" CONTRACTUAL FRAMEWORK DEDICATED TO CUSTOMER PROJECTS AND CONSTRAINTS?	P.12
15- QUELS SONT LES SERVICES HDS DISPONIBLES AVEC CLOUD SANTÉ® HYBRIDE - AWS ? - WHAT ARE THE HDS SERVICES PROPOSED BY HYBRID HEALTH CLOUD – AWS ?	P.13
16- QUI ACCÈDE AUX DONNÉES DE SANTÉ? - WHO CAN HAVE AN ACCESS TO THE HEALTH DATA ?	P.13

17- LES DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL (DSCP) SONT-ELLES INCLUES DANS LE RGPD ?

P.14

- IS THE GDPR APPLICABLE TO HEALTH DATA ?

18- QUELLES SONT LES SANCTIONS EN CAS DE NON RESPECTS DE LA RÉGLEMENTATION EN MATIÈRE DE PROTECTION DES DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL?

P.14

- WHAT ARE THE SANCTIONS FOR NON-COMPLIANCE WITH THE REGULATION ON THE PROTECTION OF PERSONAL HEALTH DATA ?

01.

QUI EST CLOUD SANTÉ® ?

Entité du groupe Euris, Cloud Santé® est opérateur de santé connectée, spécialiste de l'hébergement de données de santé.

Conformité globale :

- UE : RGPD (Règlement Général sur la Protection des Données), HDS:2018 (Hébergeur de Données de Santé) & ISO 27001:2013 (International Organization for Standardization) ;
- US : conformité HIPAA (Health Insurance Portability and Accountability Act)
- Chine : CSL (China's Cybersecurity Law).

Grâce à un modèle unique de services de marketplace, Cloud Santé® propose également une gamme complète de services et de solutions interopérables, facilitant le déploiement des projets e-santé : authentification forte, drive, archivage, sauvegarde, anonymisation, Big Data, Business Intelligence, IoT, télémédecine, CRM, PRM, etc...

02.

QUI EST AMAZON WEB SERVICES (AWS) ?

Depuis 2006, Amazon Web Services (AWS) propose une plate-forme cloud hautement fiable, évolutive et peu coûteuse, capable d'accompagner des millions d'organisations dans leur transformation.

Des dizaines de milliers de clients et de partenaires en France utilisent activement AWS pour exécuter des applications plus rapidement tout en bénéficiant d'un niveau de sécurité élevé, tel que AlloResto, Canal+, Capgemini, Claranet, Decathlon, D2SI by Devoteam, Edifixio, Engie, Fastbooking, Kartable, LafargeHolcim, Le Figaro, Leboncoin, Les Echos, Les Restos du Cœur, Mondadori France, Nexity, OpenClassrooms, PayPlug, Radio France, Scheider Electric, SNCF, Société Générale, Soitec, Teads, TF1, Veolia and

WHAT IS EURIS HEALTH CLOUD ?

Euris Health Cloud is a recognized expert in Health Digital and Cloud solutions, certified for Health Data hosting activities and managed services.

Global compliance:

- EU : GDPR compliance (General Data Protection Regulation) , HDS 2018 (Health Data Hosting Certification) & ISO 27001 :2013) (International Organization for Standardization) ;
- USA : HIPAA compliance (Health Insurance Portability and Accountability Act)
- China/PRC : CSL (China's Cybersecurity Law).

Thanks to its unique model of marketplace services, Euris Health Cloud also offers a full range of services and interconnected solutions helping the launch of E-health projects : strong authentication, drive, archiving, Big Data, Business Intelligence, IoT etc...

WHAT IS AMAZON WEB SERVICES (AWS) ?

Since 2006, AWS offers a very reliable cloud platform, evolutive and affordable, capable of supporting millions of organisations in their transformation.

Thousands of clients and partners in France are currently using AWS to execute applications more quickly and benefiting from a high level of security such as AlloResto, Canal+, Capgemini, Claranet, Decathlon, D2SI by Devoteam, Edifixio, Engie, Fastbooking, Kartale, LafargeHolcim, Le Figaro, Leboncoin, Les Echos, Les Restos du Cœur, Mondadori France, Nexity, OpenClassrooms, PayPlug, Radio France, Scheider Electric, SNCF, Société Générale, Soitec, Teads, TF1, Veolia and

PayPlug, Radio France, Schneider Electric, SNCF, Société Générale, Soitec, Teads, TF1, Veolia, et bien plus encore.

Amazon Web Services (AWS) est la plateforme cloud la plus avancée et la plus utilisée à l'échelle internationale, offrant plus de 165 services complets proposés par des centres de données aux quatre coins du monde. Des millions d'utilisateurs, notamment certaines des start-ups les plus dynamiques, des plus grandes entreprises et des agences gouvernementales principales, font confiance à AWS pour gérer leur infrastructure et leur apporter de la flexibilité, tout en réduisant leurs coûts.

Source : https://aws.amazon.com/fr/what-is-aws/?nc1=f_cc

a lot more.

AWS is the most used and most advanced at the international level, offering more than 165 full services proposed by Data Centres worldwide.

Millions of users, including some of the most active start ups, big companies and governmental agencies trust AWS to manage their hosting infrastructure offering flexibility and cost saving at the same time.

Source : https://aws.amazon.com/fr/what-is-aws/?nc1=f_cc

03.

QU'EST CE QUE L'OFFRE CLOUD SANTÉ® HYBRIDE ?

«Cloud Santé® Hybride» est la réponse de Cloud Santé® à l'enjeu et aux besoins du secteur de la santé connectée.

Il s'agit d'une plate-forme d'Hébergement de Donnée de Santé (HDS) agréée (par le ministère de la Santé Français) et certifiée (certificat HDS:2018 & ISO 27001:2013 pour l'ensemble des 6 activités et conformité HIPAA) associée à la puissance d'un cloud public.

Cette offre vous permet d'assurer à la fois la sécurité des données personnelles de santé et l'accès aux ressources technologiques nécessaires à vos projets e-santé.

La solution «Cloud Santé® Hybride» vous permet ainsi de choisir d'héberger vos données en partie ou en totalité sur un environnement cloud public ou privé.

WHAT IS HYBRID HEALTH CLOUD® ABOUT ?

Hybrid Health Cloud is Euris Health Cloud's answer to Connected Health and its specific needs.

It consists in a Health data hosting infrastructure (HDS) approved by the French Ministry of Health and certified (HDS :2018 1 ISO 27001 :2013 for all 6 HIPAA compliant activities) associated to the strength of a public cloud.

This solution allows personal health data security and access to technology resources needed in E-Health projects.

Hybrid Health Cloud solution will enable you to choose between hosting your data either in whole or in part on a public or private cloud.

04.

POURQUOI CLOUD SANTÉ® HYBRIDE - AWS ?

La solution «Cloud Santé® Hybride - AWS» s'adresse aux clients Français et Internationaux, qui souhaitent faire héberger et infogérer leur plate-forme de Santé Connectée.

«Cloud Santé® Hybride - AWS» est une plateforme d'hébergement de donnée de Santé (HDS) agréée (par le ministère de la Santé Français) et certifiée (certificat HDS:2018 & ISO 27001:2013 pour l'ensemble des 6 activités + conformité HIPAA).

Les équipes Cloud Santé® opèrent et infogèrent les infrastructures HDS.

La solution «Cloud Santé® - AWS» est composée de la manière suivante :

- Accès aux services cloud d' AWS
- Stockages des DSCP (Données de Santé à Caractère Personnel) au sein des infrastructures «privées» de Cloud Santé® ou des infrastructures cloud d'AWS
- Infogérance Cloud Santé®
- Interconnexion directe et sécurisée entre AWS & Cloud Santé®

Cette offre s'adresse aux responsables de traitement souhaitant un stockage des données en environnement public ou privé.

Cloud Santé® se charge de la mise à disposition et du maintien en condition opérationnelle de l'infrastructure matérielle, système et réseaux. L'équipe technique Cloud Santé® prend en charge l'administration et l'exploitation du système d'information utilisé pour le traitement des données de santé.

WHY HEALTH CLOUD® HYBRID AWS ?

The "Health Cloud® Hybrid - AWS" solution is aimed at French and international customers wishing to host and manage their connected health platform.

Health Cloud® Hybrid AWS is a Health Data Hosting Platform (HDS) approved (by the French Ministry of Health) and certified (HDS: 2018 & ISO 27001: 2013 certificates for all 6 activities + HIPAA compliance).

Euris Health Cloud teams operate and manage the HDS infrastructure.

The "Health Cloud® Hybrid - AWS" solution is composed as follows:

- Access to AWS cloud services
- Storage of Personal Health Data within Euris Health Cloud «private» infrastructures or AWS cloud infrastructures
- Managed services provided by Euris Health Cloud
- Direct and secure interconnection between AWS & Euris Health Cloud

This offer is intended for data controllers wishing to store data in a public or private environment. Euris Health Cloud is responsible for the provision and maintenance of the hardware, system and network infrastructure. The Euris Health Cloud technical team takes charge of the administration and operation of the information system used for the processing of Health Data.

05.

PUIS-JE HÉBERGER DES DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL (DSCP) DIRECTEMENT CHEZ AWS ?

Dans le cadre de la certification HDS d'AWS, vous pouvez héberger des Données de Santé à Caractère Personnel (DSCP) au sein des services AWS certifiés. Selon votre statut (Editeur de la solution, responsable de traitement, ...) et les opérations conduites par le responsable de traitement sur la plateforme, vous pouvez également entrer dans le champ obligatoire de la certification au titre de cette activité ou devoir la confier à un opérateur agréé ou certifié pour cette activité (activité 5).

CAN I HOST PERSONAL HEALTH DATA DIRECTLY ON AWS CLOUD ?

As part of AWS HDS certification, you can host Personal Health Data within AWS certified services. Depending on your status (solution provider, data controller ...) and the operations carried out by the controller on the platform, you may be concerned by certification obligations for this activity or have to sub-contract this activity to an authorized or certified operator (activity 5).

06.

QU'EST CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ?

Le Règlement Général sur la Protection des Données personnelles (RGPD) indique qu'une donnée à caractère personnel représente toute information relative à une personne physique, susceptible d'être identifiée, directement ou indirectement.

Source : cnil.fr

WHAT IS CONSIDERED AS PERSONAL DATA ?

The EU General Data Protection Regulation (GDPR) defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly

07.

QU'EST CE QUE LA DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL (DSCP)?

Le Règlement Général sur la Protection des Données personnelles (RGPD) donne une définition depuis avril 2016. Ce sont les données

WHAT IS CONSIDERED AS PERSONAL HEALTH DATA ?

The EU General Data Protection Regulation (GDPR) gives a definition of personal health data since April 2016.

passées, présentes et futures relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne. Des précisions sont apportées sur le site de la CNIL.

Source : cnil.fr

08.

QUI EST CONCERNÉ ET DOIT RECOURIR À UN HÉBERGEMENT DE DONNÉES DE SANTÉ (HDS) ?

L'article L.1111-8 du code de la santé publique indique que : « 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 social et 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 ».

Le Ministère des Solidarités et de la Santé précise que les personnes physiques ou morales concernées par l'hébergement de données de santé sont d'une part, les patients qui confient l'hébergement de leurs données de santé à un tiers, et d'autre part les responsables de traitements de données de santé à caractère personnel (DSCP) ayant pour finalité la prévention, la prise en charge sanitaire (soins et diagnostic) ou la prise en charge sociale et médico-sociale de personnes.

Source : sante.gouv.fr

Personal health data refers to means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

WHO IS AFFECTED AND MUST DEPLOY A SPECIFIC HEALTH DATA HOSTING SOLUTION ? (HDS IN FRANCE)

«Article L.1111-8 of the French Public Health Code specifies that: "Any natural or legal person that hosts personal health data collected during an activity of: prevention, diagnostic, social and medico-social care and monitoring for the account of natural or legal person originating the production and collection of these data on behalf of the patient itself, must be accredited or certified for this activity.»

The French Ministry of Health specifies that the legal or natural persons affected by the Health Data Hosting Solutions, are on one hand the patients that assign the hosting of their personal health data to a third party, and on another hand the entities responsible for the handling of personal health data with as a finality: the prevention, the healthcare (care and diagnostic), the social or medico-social care of the persons.

09.

QU'EST-CE QU'UN TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL (DSCP)?

L'article 2 de loi Informatique et Libertés définit les traitements de données personnelles comme « toute opération ou tout ensemble d'opérations portant sur des données personnelles quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

10.

QUI EST LE «RESPONSABLE DE TRAITEMENT» ?

L'article 4 du RGPD définit le responsable de traitement comme étant « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Ainsi, pour déterminer qui de la société éditrice du logiciel ou de l'utilisateur du logiciel (professionnel ou établissement de santé) a la qualité de responsable de traitement, il convient d'identifier qui détermine les finalités et les moyens du traitement opérés par le biais du logiciel.

11.

L'ÉDITEUR DE LOGICIEL EST-IL «RESPONSABLE DE TRAITEMENT» ?

«La CNIL a eu l'occasion de considérer à de très nombreuses reprises qu'en principe l'éditeur d'un logiciel n'est pas le responsable du traitement

WHAT DO WE MEAN BY PROCESSING PERSONAL DATA ?

According to article 2 of the French Data Protection Law (loi informatique et Libertés)* «handling personal data refers to any processing of personal data whatever system or process used, and essentially collecting, saving, structuring, adapting, modifying, extracting, consulting, using, communicating etc or any other form of handling including interconnection, locking, erasing or destroying.»

**this translation is informative only and is not a legal translation nor has any legal value...*

WHO IS THE DATA CONTROLLER ?

Under article 4 of the GDPR 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Therefore, to determine who between the software editor and the software user is the data controller, it is important to determine how and why data are processed through the software.

**this translation is informative only and is not a legal translation nor has any legal value...*

IS THE SOFTWARE PUBLISHER THE « DATA CONTROLLER » ?

The French data protection body (CNIL) has had to consider on a number of occasions that in principle, the software publisher is not responsible

mis en œuvre à partir de ce logiciel : l'exemple le plus fréquemment repris est celui du médecin ou de l'établissement de santé qui utilise un logiciel pour gérer le cabinet médical ou pour administrer les dossiers médicaux édités par un prestataire tiers éditeur, dans les deux cas, c'est bien le médecin ou l'établissement de santé qui est « responsable du traitement » mis en œuvre à partir du logiciel utilisé.

En l'espèce, il y a lieu de comprendre que les responsables de traitement seront les clients de l'éditeur, lui-même client de l'hébergeur de données de santé, et qu'en conséquence ses responsables de traitements sous contrat avec l'éditeur pourraient être situés soit sur le territoire français, soit sur d'autres territoires [...].»

12.

QUEL EST LE RÔLE DE L'HÉBERGEUR DE DONNÉES DE SANTÉ ?

L'article L.1111-8 du code de la santé publique relatif à l'hébergement de données de santé a pour objectif d'organiser et d'encadrer la conservation et la restitution des données de santé à caractère personnel (DSCP), dans des conditions propres à garantir leur confidentialité et leur sécurité.

Par cet encadrement, le législateur souhaite garantir la confiance dans les tiers auxquels des structures et des professionnels des secteurs sanitaire, social et médico-social confient les données de santé qu'ils produisent ou recueillent, notamment en mesurant l'impact de l'activité du prestataire sur la protection des données, au travers des critères de sécurité à l'état de l'art « disponibilité, intégrité, confidentialité et auditabilité (DICA) » notamment visés par l'ANSSI et les normes ISO.

Cette confiance dans les tiers agissant pour le compte de ces acteurs sanitaires et sociaux et médico-sociaux est donnée au travers de l'obligation d'être agréé et/ou certifié « HDS ».

Source: Document « Explication du champ d'application du cadre juridique de l'hébergement de données de santé par le ministère chargé de la Santé, représenté par la Délégation à la stratégie des systèmes d'information de santé » édité par le Ministère des solidarités et de la santé

for the data processing done using the software. One common example would be a practitioner or health care facility using a software to manage the medical practice or medical files edited by a third party publisher; in both cases the data controller would be the practitioner or the health care facility using the software.

Clients of the publisher will be the data controller, the editor himself being the client of the legal entity hosting the health data and therefore, the data controllers contracting with the publisher could be located on the territory of France or any other territory.

WHAT IS THE ROLE OF THE HEALTH DATA HOSTING PROVIDER ?

The main objective of Article L.1111-8 of the french public health code on health data hosting is to regulate conservation and restitution of personal health data in such conditions as to guarantee safety and confidentiality.

This is meant to secure the trust in any third parties to which healthcare, social and medico-social structures and professionals transfer the health data they produce or collect, in particular by measuring the impact of the service provider activity on the protection of data, through security criteria «availability, integrity, confidentiality and auditability».

This trust in third parties acting on behalf of these healthcare and social and medico-social stakeholders is given through the obligation to be approved and / or certified «HDS».

13.

QUELLES SONT LES ACTIVITÉS DE LA CERTIFICATION HDS ?

Les activités de la certification HDS sont les suivantes :

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.
3. Mise à disposition et maintien en condition opérationnelle de la plateforme d'hébergement d'application 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. Sauvegarde externalisée des données de santé.

14.

QUI CONSTRUIT UN CADRE CONTRACTUEL HDS GLOBAL DÉDIÉ AUX PROJETS ET AUX CONTRAINTES CLIENTS ?

Dans le cadre de la solution Cloud Santé® Hybride, Cloud Santé® met en place un cadre contractuel HDS global suivant les contraintes des clients tout en les assistant dans le respect de la réglementation. Un accompagnement

WHAT ARE THE ACTIVITIES COVERED BY THE HDS CERTIFICATION ?

1. The provision and maintenance in operational condition of physical sites for hosting the Hardware infrastructure of the information system used to process health information.
2. The provision and maintenance in operational condition of the hardware infrastructure of the information system used to process health information.
3. The provision and maintenance in operational condition of the virtual infrastructure of the information system used to process health information.
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 health data information.
6. Outsourced backup of health data.

WHO BUILDS A GLOBAL "HDS" CONTRACTUAL FRAMEWORK DEDICATED TO CUSTOMER PROJECTS AND CONSTRAINTS ?

Within the framework of Health Cloud® Hybrid solution, Euris Health Cloud implements a global HDS contractual framework according to the constraints of the customers while assisting them in their compliance with the regulation. The

par les équipes Cloud Santé® tout au long du processus de déploiement, permet de créer un projet personnalisé et en adéquation avec les caractéristiques clients.

Support of Euris Health Cloud teams throughout the deployment process, enable the creation of a customized project and in line with customer specificities.

15.

QUELS SONT LES SERVICES HDS DISPONIBLES AVEC CLOUD SANTÉ® HYBRIDE - AWS ?

Le catalogue de service Cloud Santé® et l'ensemble des services certifiés ISO 27001 fournis par AWS (*).

Cloud Santé® propose un catalogue complet de services prêts à l'emploi et implémentés en étroite collaboration avec nos partenaires : accompagnement et conseil, authentification forte, bastion, drive, archivage, sauvegarde, anonymisation, Big Data, Business Intelligence, IoT, télémédecine, CRM, PRM etc...

Chaque partenaire de Cloud Santé® a été sélectionné parmi les meilleures entreprises de son secteur. La synergie entre les sociétés permet plus d'innovation et de services adaptés répondant aux besoins de tous les acteurs de l'écosystème de santé.

WHAT ARE THE HDS SERVICES PROPOSED BY HYBRID HEALTH CLOUD – AWS ?

The services proposed by Health cloud and AWS ISO 27001 certified services.

Health Cloud offers a wide range of services ready to be used and integrated in close cooperation with its partners: support and consulting, strong authentication, bastion, drive, archiving, backup, anonymization, Big Data, Business Intelligence, IoT, telemedicine, CRM, PRM etc...

Each Health Cloud partner has been selected among the best companies in their field. The synergy between the companies allows more innovation and adapted services answering the needs of all the actors of healthcare ecosystem.

16.

QUI ACCÈDE AUX DONNÉES DE SANTÉ?

Les données de santé peuvent être consultées par le patient et le professionnel de santé. La collecte de données de santé et l'exploitation de bases les traitant sont soumises à une réglementation HDS très stricte, définie par le code de la santé publique modifié par Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel, et destinée à garantir la confidentialité, la sécurité de ces données et à assurer la protection de la vie privée du patient.

WHO CAN HAVE AN ACCESS TO THE HEALTH DATA ?

The Health Data can be accessed by the patient and the Healthcare Professional. The collection of health data and the exploitation of medical device data are subjected to a very strict regulation under French regulation (Decree n° 2018-137 of 26 02 2018 related to health personal data hosting and intended to ensure confidentiality, the security of such data and the protection of the patient's privacy.

17.

LES DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL (DSCP) SONT-ELLES INCLUES DANS LE RGPD ?

Les réglementations HDS (Hébergement de Données de Santé) et RGPD (Règlement Général sur la Protection des données) sont complémentaires. Le RGPD définit les obligations générales comme la nomination d'un DPO, la réalisation d'analyse d'impact sur la vie privée ou encore la déclaration des incidents de sécurité. La réglementation HDS précise et renforce les mesures de sécurité à mettre en œuvre et les rend applicables. Les données de santé sont des données à caractère personnel «particulières» car considérées comme sensibles. Elles font à ce titre l'objet d'une protection particulière par la réglementation (code de la santé publique, agrément et certification pour l'hébergement de données de santé à caractère personnel, etc...)

18.

QUELLES SONT LES SANCTIONS EN CAS DE NON RESPECTS DE LA RÉGLEMENTATION EN MATIÈRE DE PROTECTION DES DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL ?

En cas de non-respect du Règlement Générale sur la Protection des Données (RGPD) :

Les sanctions sont réparties en deux groupes en fonction de la durée, la nature et la gravité de la violation.

Lorsqu'il s'agit d'un des manquements aux obligations suivantes :

- Les obligations incombant au responsable du traitement et au sous-traitant
- Les obligations incombant à l'organisme de certification
- Les obligations incombant à l'organisme chargé

IS THE GDPR APPLICABLE TO HEALTH DATA ?*

The General Data Protection Regulation (GDPR) and the French legislation on Health Data hosting (HDS) are complementary.

GDPR defines general obligations such as appointing a DPO, conducting a privacy impact assessment or notifying security incidents. The French legislation on Health Data hosting imposes additional security measures. Health data are treated as sensitive data and as such are subject to very strict rules in order to maintain the privacy of the persons concerned and their data. HDS certification can be used as a GDPR compliancy tool.

WHAT ARE THE SANCTIONS FOR NON-COMPLIANCE WITH THE REGULATION ON THE PROTECTION OF PERSONAL HEALTH DATA ?

If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

Infringements of the following provisions shall be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the obligations of the controller and the processor
- (b) the obligations of the certification body

du suivi des codes de conduite.

Une amende d'un montant de 2% du chiffre d'affaires mondial pour les entreprises ou 10 millions d'euros peut être appliquée.

Lorsqu'il s'agit d'un des manquements aux obligations suivantes :

- L'obligation de consentement de la personne concernée avant collecte, traitement ou stockage des données personnelles
- Les autres droits des personnes concernées
- Les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale
- Toutes les obligations découlant du droit des Etats membres
- Le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle.

Une amende qui correspond à 4 % du chiffre d'affaires mondial s'agissant des entreprises ou 20 millions d'euros peut être appliquée.

En cas de non respect de la réglementation liée à la protection des Données de Santé à Caractère Personnel (DSCP) :

Les sanctions pénales prévues (articles 1115-1 et 1115-2 du Code de la santé publique) en cas d'hébergement de données de santé à caractère personnel (DSCP) sans agrément ou certification HDS :

- Trois ans d'emprisonnement et 45 000 euros d'amende;
- Interdiction pour une durée de 5 ans ou plus d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;
- Placement, pour une durée de 5 ans ou plus, sous surveillance juridique ;
- La fermeture définitive ou pour une durée de cinq ans au plus des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
- L'exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus ;
- L'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.»

(c) the obligations of the monitoring body

Infringements of the following provisions shall be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent;

(b) the data subjects' rights;

(c) the transfers of personal data to a recipient in a third country or an international organisation;

(d) any obligations pursuant to Member State law;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority or failure to provide access.

Non-compliance with an order by the supervisory authority shall be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Breach of Article L.1111-8 of the Public Health Code is sanctioned by up to 3 years imprisonment and a fine of € 45,000 in case of individuals and € 225,000 in case of legal entities.

Processing of personal data in such circumstances may also be sanctioned by the French data protection authority (the "CNIL"), that can impose a fine of up to € 3 million (and after 25 May 2018, up to €20 million or 4 % of the worldwide turnover), as well as an injunction to cease processing. Sanctions are made public. The CNIL has already issued a sanction in relation a health data hosting service provider.

Breaches to data protection regulations or to professional secrecy can also give rise to criminal fines.

It is essential that Article L.1111-8 be taken into account when dealing with certain types of health data of French residents.

Source:<https://www.securityprivacybytes.com/2018/05/france-issues-new-rules-for-the-accreditation-of-health-data-hosting-services-providers/>



Euris Health Cloud (Cloud Santé®)

116 rue de Silly, 92100 Boulogne, Paris, France
Tél. +33 (0)1 55 95 00 50 - Email: commercial@euris.com
www.euris.com

© Euris Health Cloud (Cloud Santé®) - All rights reserved