euris
health cloud®

Compliance & Security
for the Healthcare and Life Sciences Sector

Vision & Solutions to tackle current challenges

euris health cloud (cloud santé) - 116 rue de Silly - 92100 Boulogne, Paris – France – Tel. : +33 (0)1 55 95 00 50

INDEX

1. EXECUTIVE SUMMARY

The digitization of personal health information (PHI) through electronic health record (EHR) has become widespread due to their efficiency in terms of cost, storage, processing, and the subsequent quality of delivering patient care. However, security concerns remain one of its major setbacks.

On the one hand, in order to handle EHR, healthcare actors need to comply with their local government security regulations applied to health data management. These regulations control to which extent health data can be processed, transmitted, stored, as well as define how misuses are addressed.

On the other hand, as on premise infrastructures managing patient data are increasingly moving to the cloud and the new priority of cloud service providers are setting software-enabled cloud services, the healthcare industry faces new exigencies in terms of security, ethics and performance, which directly have an impact on how compliance has to be implemented, measured and supervised.
The multiplicity of regulations accentuates the complexity and most healthcare actors don’t even know where to start.

This paper presents **recommendations to setting a compliant IT health infrastructure based in our field experience deploying projects around the world**, either on private cloud infrastructure environment, or the Hybrid cloud infrastructure implemented within our partnership with AWS.

2. HEALTH DATA COMPLIANCE & SECURITY: A KEY REQUISITE FOR PATIENT SAFETY

2.1. HEALTH DATA COMPLIANCE, A GROWING FIELD WITHIN THE HEALTHCARE & LIFE SCIENCES INDUSTRIES

The democratization and increase of digital services processing personal healthcare data (PHD) require the implementation of secure, reliable and strict protocols allowing all stakeholders to access secure data.

In order to tackle above challenges and regulate the security compliance of health platforms, the security of EHR is now an integral part of the legislation in many countries such as HDS (Health Data Hosting) in France, HIPAA in the USA, and CSL in China.

The design and implementation of health applications need to comply with regulations aligned to each country legislation, in order to ensure the protection of health data and thus avoid any form of prejudice to patients.

These regulations aim at addressing the security concerns around EHR by governing how health data are processed and stored, granting specific rights to patients (e.g., requesting amendments, informing in which way their data are used/shared, restricting disclosure), defining how misuses and improper disclosures are addressed (e.g., fines and penalties) as well as promoting the initiation of international standards.

Additionally, as protected data is growing exponentially, more systems need to become compliant in a shorter period of time, with a deeper attention to reduce new attack risks and maintain/upgrade their innovation capabilities.

Healthcare organizations should then rely on reliable compliance & cybersecurity expertise.

2.2. HEALTH DATA SECURITY AND COMPLIANCE SOLUTIONS FOR HEALTHCARE & LIFE SCIENCES ORGANIZATIONS: OUR PROVENEURIS HEALTH® CLOUD EXPERTISE

Euris Health Cloud® is an international Health Data Cloud provider, based in France, dedicated to healthcare & life sciences industry, **specialized in Health Data compliancy & security**.

In order to ensure the protection of personal health data within the infrastructures managed, Euris Health Cloud® guarantees compliance with the main regulatory frameworks applied in the European Union, United States and China.

In Europe, Euris Health Cloud disposes the HDS: 2018 certification for hosting and information management of health data as well as the ISO/IEC 27001:2013 certification.

Introduced in 2018 by the French governmental agency for health, ASIP Santé (Agence Française de la Santé Numérique), the HDS certification provides a framework to strengthen the security and protection of personal health information. HDS represents the regulation of reference for any entity providing hosting of health data when setting up health and safety systems in France.

Euris Health Cloud® disposes the entirety of the two components available in the certification: Infrastructure Host and HDS hosting outsourcing, covering **all six possible HDS activities** of the HDS certification framework

HDS certification brings together several international ISO standards to ensure the best quality and management of IT risks. Thus, an HDS certified information system is the guarantee of meeting the requirements of the standards:

- ISO 27001 "Information Systems Security Management System"
- ISO 20000 – 1 "Service Quality Management System"
- ISO 27018 "Protection of personal data"

As such, the HDS certification is one of the **fullest and stricter legal frameworks** conceived to **secure and protect personal health data applied worldwide**.

By being HDS certified, Euris Health Cloud® becomes the first global, **secure, reliable and accredited cloud dedicated to connected health in Europe**. The achievement of the HDS certification validates the capabilities of Euris Health Cloud® to ensure data confidentiality, data security, business continuity in alignment with the General Data Protection Regulation (GDPR) applied in Europe, and tailored support thanks to our **multi-territory certified infrastructure**.

CHART 1: Overview of French HDS certification, a worldwide reference in terms of health data protection

Information Security Management System ISO 27001 Certified Hébergement de Données de Santé HDS 123456 Certified	Euris Health Cloud® is certified for Health data infrastructure hosting activities and managed services, which consists in secure hosting and managing services in its datacenters and in hybrid cloud with AWS of personal health data, collected or produced by editors, services providers or patients. More precisely, Euris Health Cloud® achieved certification in the following areas: 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 information;** 6. The backup of the health information

As for the **United States** market, Euris has achieved full compliance with the HIPAA current regulation, covering all the cloud services activities scope.

Regarding the **Asia** region, local regulations applied to the health data in China (Cyber Security Law, CSL) require the management and hosting of personal data of Chinese citizens on Chinese territory.

Euris Health Cloud's infrastructure complies with the CSL regulatory framework and therefore can host health applications and services in a fully secure environment, meeting the compliance, integrity and data confidentiality exigencies required in China.

By integrating this full compliance approach, Euris Health Cloud® helps its partners and clients (pharmaceutical and device medical companies, health insurance companies, health services providers) processing personal health data to innovate with confidence, maximize opportunities and drive healthcare forward.

For companies using Amazon Web Services (AWS) solutions, Euris Health Cloud® offers:

- Expertise as an approved and certified Health Data Hosting Provider (HDS certificate: 2018 & ISO 27001: 2013 for all 6 activities in Europe; HIPAA in USA; CSL in China) to ensure simplicity and security in the implementation of a health platform.
- A health data hosting combined with the power- scalability - effectiveness of AWS cloud to develop innovative e-health projects.
- A compliance verified several times a year by external audit companies: technical, quality and cybersecurity audits.
- A specific compliance in accordance with the SNDS (French National Health Data System of 60 million people) safety reference.

Euris has developed the « **Health Cloud® - Hybrid AWS** » solution to assure that personal healthcare data are:

- **Available**: accessible and usable by its authorized recipient at the place and time specified.
- **Integrated**: alterable only by authorized persons and according to a pre-established process.
- **Confidential**: only accessible to authorized persons.
- **Auditable**: all modifications or movements of the data are tracked.

Our teams is focused on proximity to our customers throughout the implementation of the project, thanks to a dedicated project coordinator putting customer satisfaction at the core of the deployment.

Our teams will operate and manage each client's « Health Cloud® - Hybrid AWS » HDS infrastructure.

The goal of Euris Health Cloud® & AWS together: serve the Heathcare system by consistently providing the most performant healthcare infrastructure and excellent customer service.

Euris Health Cloud® combined with AWS' advanced solutions and capabilities offers the best compromise to monitor Personal Healthcare Data accordingly to our clients' requirements.

For more than 20 years, Euris Health cloud® supports the deployment of innovative services for all healthcare stakeholders in over 30 countries.

Euris Health Cloud®- Hybrid AWS compliant & secure offer increase the security of health data:

- By considerably reducing the exposure to legal and financial risks thanks to our EEC[1] HDS compliance carried under AWS guaranteeing the highest level of security of your health data.
- Allowing our clients to focus on their business development. **Each client can think globally and easily Plan, Deploy, Scale up its project to foster business development locally or worldwide.**

[1] *European Economic Community*

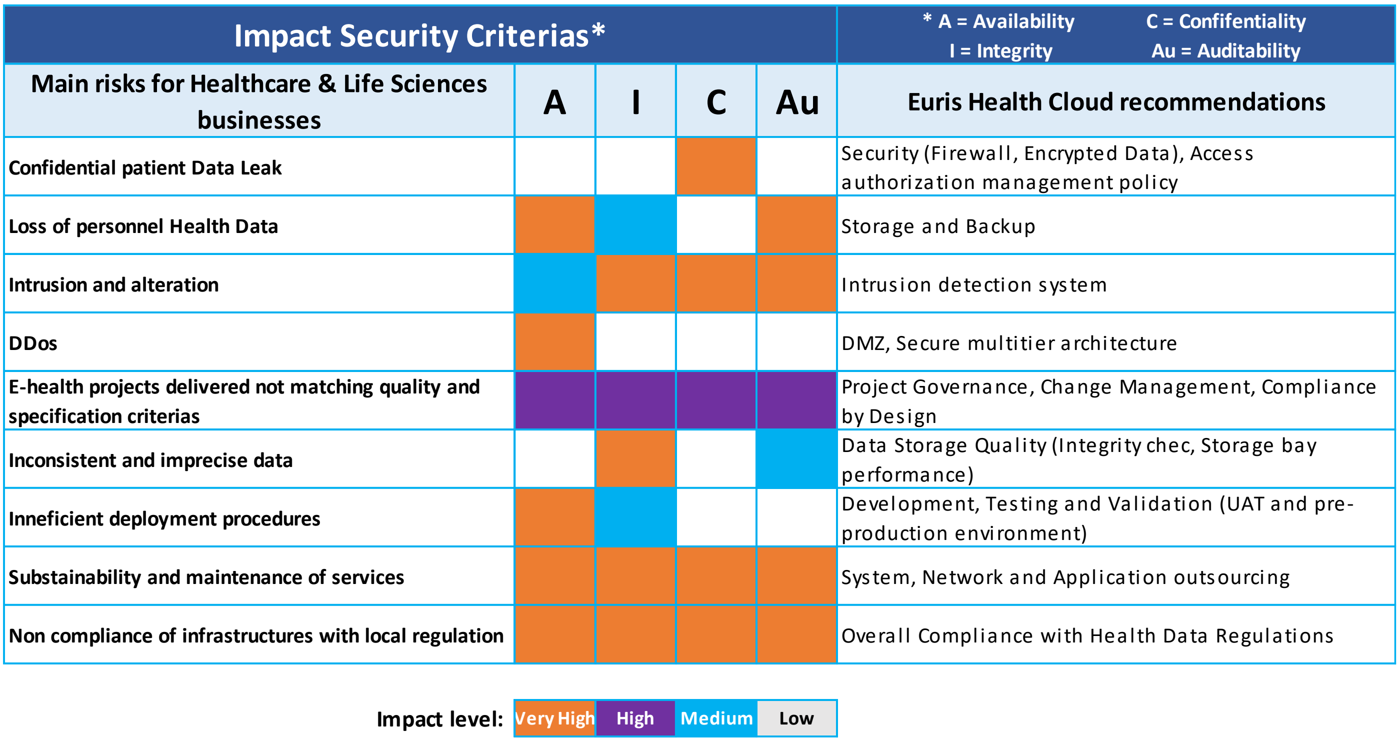
2.3. CLOUD COMPLIANCE EFFECTIVE MODELS

The implementation of legal regulations listed in the precedent section should limit the impact on users (e.g., doctors) given the special context in which they operate. For instance, these applications should remain easily and quickly accessible to healthcare practitioners in order to ensure efficient patient care. They should also be accessible to information system administrators in a maintenance perspective so as to ensure their availability and continuation of services.

However, these flexibilities introduce security risks relative to confidentiality and integrity of data. The compromise between the efficiency of delivering healthcare services and the protection of patients' data lies in maintaining the accessibility of applications and setting up monitoring and management mechanisms to handle security compliance at runtime. Adopting such a proactive approach for compliance management in a sensitive health environment is challenging since it requires monitoring as well as automatically reacting to non-compliance by performing actions on the environment at runtime.

Particularly, it entails characterising, monitoring, and managing the following four security areas: confidentiality, integrity, availability, and traceability (chart 2).

CHART 1: Overview of French HDS certification, a worldwide reference in terms of health data protection



Impact Security Criterias*					* A = Availability C = Confifentiality I = Integrity Au = Auditability
Main risks for Healthcare & Life Sciences businesses	**A**	**I**	**C**	**Au**	**Euris Health Cloud recommendations**
Confidential patient Data Leak			🟧		Security (Firewall, Encrypted Data), Access authorization management policy
Loss of personnel Health Data	🟧	🟦		🟧	Storage and Backup
Intrusion and alteration	🟦	🟧	🟧	🟧	Intrusion detection system
DDos	🟧				DMZ, Secure multitier architecture
E-health projects delivered not matching quality and specification criterias	🟪	🟪	🟪	🟪	Project Governance, Change Management, Compliance by Design
Inconsistent and imprecise data		🟧		🟦	Data Storage Quality (Integrity chec, Storage bay performance)
Inneficient deployment procedures	🟧	🟦			Development, Testing and Validation (UAT and pre-production environment)
Substainability and maintenance of services	🟧	🟧	🟧	🟧	System, Network and Application outsourcing
Non compliance of infrastructures with local regulation	🟧	🟧	🟧	🟧	Overall Compliance with Health Data Regulations

Impact level: 🟧 Very High 🟪 High 🟦 Medium ⬜ Low

Authors: Lourdes Chabrol; Yassine Zaikh; Pierre Bessemoulin | Euris Health Cloud®. 2022.

To be most effective, a cloud compliance management system needs to be designed to fit the specific requirements of the industry. For healthcare compliance, a tool should meet the needs of HIPAA, GDPR, GxP, and HDS (for projects deployed in France).

Based in our experience, our team recommend **the adoption of a "global" compliance approach to the tools and solutions used for managing data on the public cloud, based on a three-step check list to securing Health Compliance environments** on Euris Health Cloud® & AWS solutions.

2.5. GLOBAL COMPLIANCE & SECURITY APPROACH - THREE-STEP CHECK LIST

2.4.0. *Deep technical evaluation of level of compliance with local regulations*

Let's take the context applied in the United States as example.

Health data hosting solutions managing personal health information, provided within the Euris Health Cloud® AWS Hybrid Cloud offer guarantees compliance with HIPAA regulatory framework applied in the U.S.

In other words, the infrastructure is secure enough to "pass" the different security, privacy and policy procedures, "controls", aroused once the digital health application/service manages personal health information (storing, processing and transmission).

2.4.1. *A Methodical Implementation Approach*

Once a healthcare stakeholder decides to implement a Hybrid Euris Health Cloud® AWS environment to host its application and health data in compliance with HIPAA, HDS & GDPR regulations, our team deploys the following missions:

- **SOW 1: Study and proposal of a global «HDS» technical architecture/solution (multi territory) based on AWS and Euris Health Cloud tools and solutions.**

  SOW 1 - Outcome Results
  The scalability criterion becomes essential. The Euris Health Cloud® Hybrid AWS offer provides a secure and flexible infrastructure that adapts to the client's growth. Platform can scale up locally or at the international level.

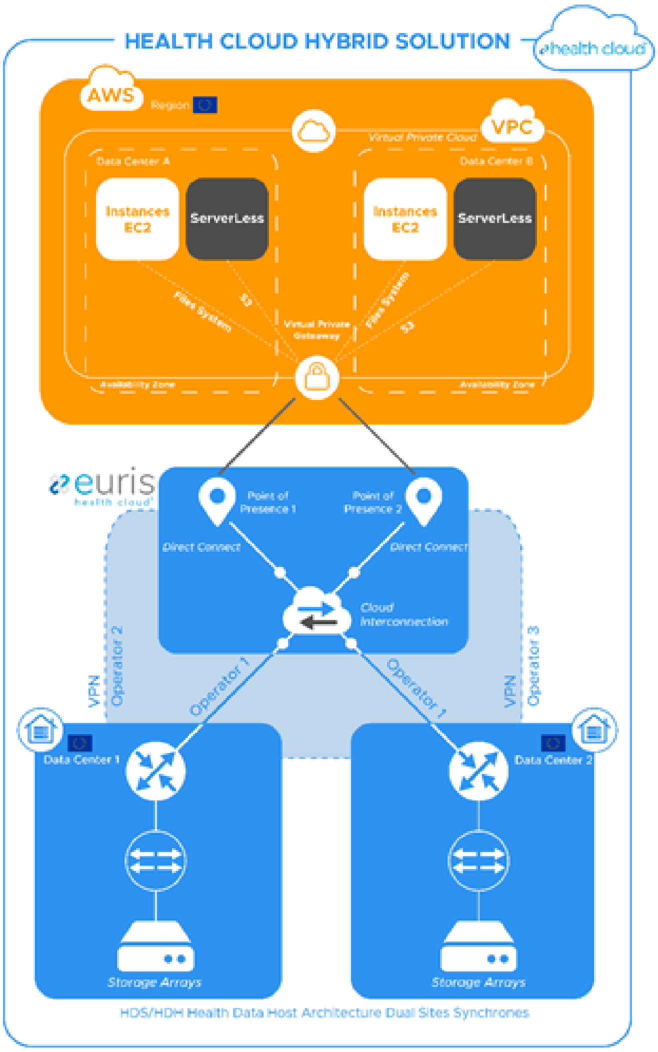
  Hereby an example of services and deliverables included in this phase

- **SOW 2: Project implementation and exploitation of clients' Application on Hybrid HDS AWS platform (BUILD & RUN)**
  SOW 2 - Outcome Results

The platform aims to operate all the components of the HDS client's architecture.

- Euris Health Cloud® leads the contract with the client and manage the necessary subcontractors for the HDS platform with AWS
- Euris handles the system and network outsourcing of the Euris Health Cloud® Hybrid HDS AWS platform.
- Euris Health Cloud® manages the administration console (AWS) and provides accesses to allow client's final users to operate

CHART 3. Example of a Hybrid Euris Health Cloud® AWS infrastructure deployed



Each architecture disposes of specific components and services.

Among most commonly AWS services requested for the health data collect and treatment we have:

- EC2 - Amazon Elastic Compute Cloud: Web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

- EBS - Amazon Elastic Block Store: Easy to use, high-performance, block-storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction intensive workloads at any scale.

- EFS - Amazon Elastic File System: Simple, serverless, set-and-forget, elastic file system that lets you share file data without provisioning or managing storage.

- VPC - Amazon Virtual Private Cloud: Service that lets you launch AWS resources in a logically isolated virtual network that you define.

- AWS WAF - Web Application Firewall: Web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources.

- KMS - AWS Key Management Service: Create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys.

- SES - Amazon Simple Email Service: Cost-effective, flexible, and scalable email service that enables developers to send mail from within any application. You can configure Amazon SES quickly to support several email use cases, including transactional, marketing, or mass email communications.

- RDS - Amazon Relational Database Service: Makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups.

- ACM - AWS Certificate Manager: Service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.

- Amazon CloudFront: Fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

- AWS Autoscaling: Monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.

To discover more about full range of services proposed by AWS, click here

Supervision, stockage, ticketing system and Bastion Access are hosted on the Euris Health Cloud® platform.

In addition to the above tools, Euris propose specific services focused on HDS / ISO 27001 / HIPAA compliance:

- AWS Config: provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.
- Trusted Advisor: AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices. Trusted Advisor checks help optimize your AWS infrastructure, improve security and performance, reduce your overall costs, and monitor service limits.
- Cloud Watch: Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.
- IAM: AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

2.4.2. *Deploy measures to enhance Security of Cloud configurations*

The digitization of healthcare has revolutionized the efficiency of the industry in terms of storage, transmission, and processing capabilities as well as in terms of quality, cost, and time effectiveness of patient care.

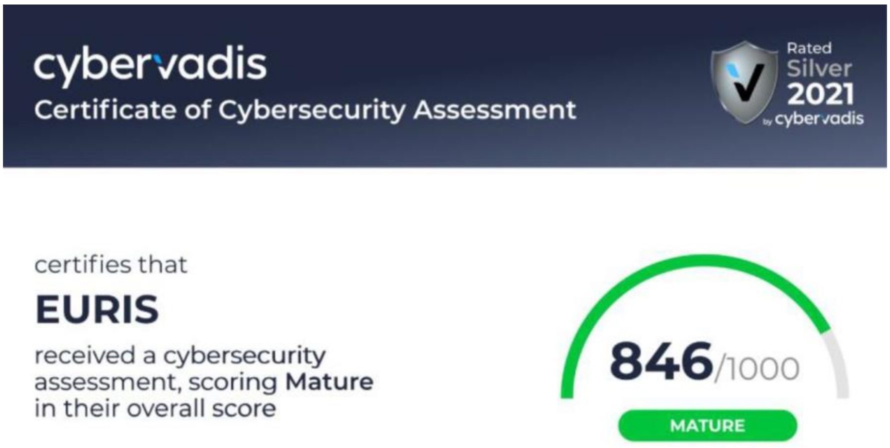
While the benefits of EHR are considerable, security concerns have remained one of the major barriers hindering its adoption. This is because of the evolving cyber threats and the subsequent need for new measures to ensure the security of the data.

Euris Health Cloud’s information security management system meets the requirements of the main applicable international standards, in particular NIST Cybersecurity and ISO 27001.

In terms of security, 4 axes of action are implemented by our teams:

IDENTIFY	Identify the data assets that should be protected. Identify the risks to which the organization is exposed and decide on the **data privacy** measures to be implemented to cover the major risks. Euris Health Cloud® manages continuous improvement through a risk analysis for the optimization of our measures of interest of potential vulnerabilities.
PROTECT	Implement security measures that help limit or contain the impacts associated with a cybersecurity event. • Euris Health Cloud proposes a secure infrastructure providing a SLA of 99.9% • Guarantee confidentiality of patient health data: Euris provides a multi-territory hosting infrastructure compliant with certifications applied for personal health data: EU (HDS / GDPR / ISO27001), US (HIPAA), and China (CSL). • Strong authentication applied. All access to infrastructure resources is recorded and is subject to periodic audits. • Daily control via monitoring and supervision of our platforms
DETECT	• Develop and implement the measures that make it possible to take the necessary actions following the occurrence of a security event. • Vulnerability detection and compliance monitoring.
IMPLEMENT	Develop and implement the measures that make it possible to take the necessary actions following the occurrence of a security event. • Euris Health Cloud’s information security management system displays the «Mature» status label following the audit of CyberVadis, a specialist in cybersecurity. CyberVadis compliance certified by PwC Certification B.V, an independent and accredited certification body: www.cybervadis.com/us/trust-center/ (see Chart 4 to refer to the official accreditation obtained by Euris Health Cloud®)

CHART 4: Cybersecurity Maturity Assessment. Score “Mature” obtained by Euris Health Cloud®. March 2021.



cybervadis
Certificate of Cybersecurity Assessment

Rated
Silver
2021
by cybervadis

certifies that
EURIS
received a cybersecurity assessment, scoring **Mature** in their overall score

846/1000
MATURE

2.6. EURIS HEALTH CLOUD®CONSULTING & INTEGRATION SUPPORT

In addition of its compliance and security offering with AWS services, Euris Health Cloud® develops a rich ecosystem of Advisory and Consulting partners in Europe and in Asia.

Each partner was selected for its solution-oriented mindset to solve client’s difficulties, in order to facilitate their project in conformity with the local regulation and highest level of health data security.

Our partners can assist you for a local or through several geos for:

- Legal counsel on data regulation,
- Medical device – software as medical device conformity,
- Go-To-Market strategy,
- Project migration on AWS (E.g. On premise to Hybrid Cloud AWS, from Microsoft to AWS, from Oracle to Microsoft, …),
- AWS awareness and training,
- AWS architecture definition and optimization,

Euris Health Cloud® and partners aligned their project management methodology to accompany client’s projects throughout its value chain.

Discover our worldwide partners and solutions provided here

2.7. CONCLUSIONS

Compliance is a key factor in Healthcare as it guarantees that legal, ethical and quality standards are met and communicated throughout the entire healthcare organization.

Compliance requires continuous monitoring of stablished configuration to ensure infrastructure validity and patient safety. This is why healthcare industry needs highly customizable & scalable solutions, adapted to different regulatory frameworks.

Since the issues tackled in this paper are similar for all applications handling EHR, our propositions are generic, global, and applies to all current health data regulations on EHR.

Euris Health Cloud® provides an architecture that guarantees both the security of personal healthcare data and the access to the technological resources necessary for the exploitation and analysis of the data.

If your organization needs to deploy a full compliant system, we invite you to discover current solutions proposed by Euris Health Cloud® and AWS. You can reach our Euris Health Cloud® dedicated team here.

2.8. RESOURCES

- *Risk Analysis Based Security Compliance Assessment and Management for Sensitive Health Data Environment. Umar Ozeer & Badara Pouye. Euris Health Cloud. April 2021.*
- *French Health Data Hosting Regulation: https://esante.gouv.fr/labelscertifications/hebergement-des-donnees-de-santé.*
- *ASIP Référentiel d'Accréditation HDS - HDH accreditation reference system. June 2018. https://esante.gouv.fr/sites/default/files/media_entity/documents/asip---referentiel-daccreditation-hds----v1.1---en.pdf*
- *HIPAA Compliance Assistance. Summary of the HIPAA Privacy Rule. Office for Civil Rights, 2003*
- *Health Level - 7 Compliant Clinical Patient Records System. In Proceedings of the 2004 ACM Symposium on Applied Computing, SAC '04, page 259–263. Association for Computing Machinery, 2004. Jagbir S. Hooda, Erdogan Dogdu, and Raj Sunderraman.*
- *FAQ – Find answers to the most frequently asked questions about health data hosting: https://www.euris.com/health-data-hosting/faq/*
- *Euris Health Cloud® Hybrid for Healthcare: https://www.euris.com/health-data-hosting/hybrid-cloud/*
- *FAQ Health Data Hosting & Health Cloud ® Hybrid Aws. 2019, Co-authors: Euris Health Cloud HQ team and AWS France.*

2.9. ABOUT EURIS HEALTH® CLOUD

Euris is an international IT group dedicated to healthcare & life sciences industry. We provide a complete chain of value from digital business solutions (All-in-one CRM and multichannel medical promotion) to certified health data hosting solutions.

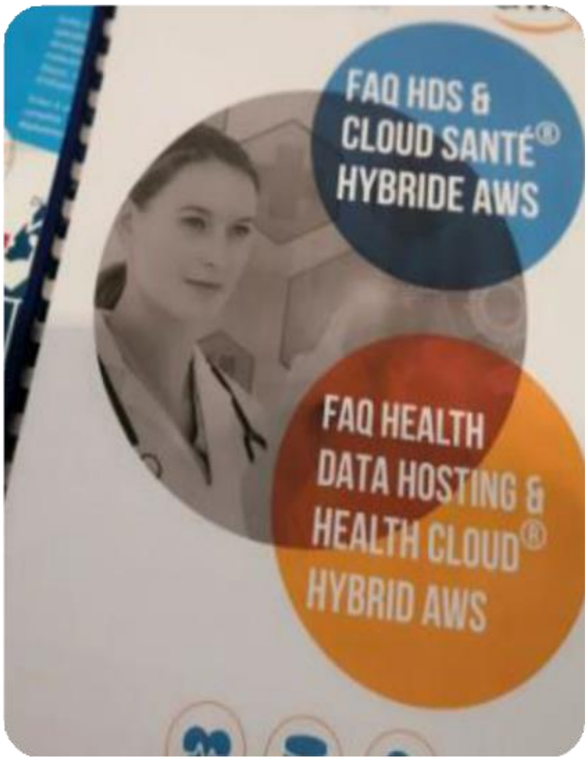
For more than 20 years, Euris supports the deployment of innovative services & technologies for all healthcare stakeholders: Life Sciences companies, healthcare insurers, healthcare SaaS providers & medical devices companies.

Website: www.euris.com

Follow Us:

Our successful partnership with AWS in images:

- https://www.euris.com/news/euris-and-aws-at-the-service-of-a-secure-health-data-system/
- https://www.euris.com/news/aws-hybrid-cloud-event/
- https://www.euris.com/fr/news/webinar-e-sante-conformite-hds-cloud-hybride-impact-benefices-pour-lindustrie-de-sante/
- https://www.euris.com/fr/news/village-cloud-sante-paris-healthcare-week-2019/
- https://www.euris.com/news/ehealth-networking-workshop-4th-october/



health cloud® HYBRID

aws

ALL THE POWER OF A HYBRID CLOUD AT THE SERVICE OFYOUR HEALTH IT PROJECTS

YOUR CONTACTS:

Marketing & Communication: Lourdes Chabrol | lourdes.chabrol@euris.com
Head of e-Health Partnerships: Pierre Bessemoulin | pierre.bessemoulin@euris.com
CEO: Pedro Lucas | pedro.lucas@euris.com