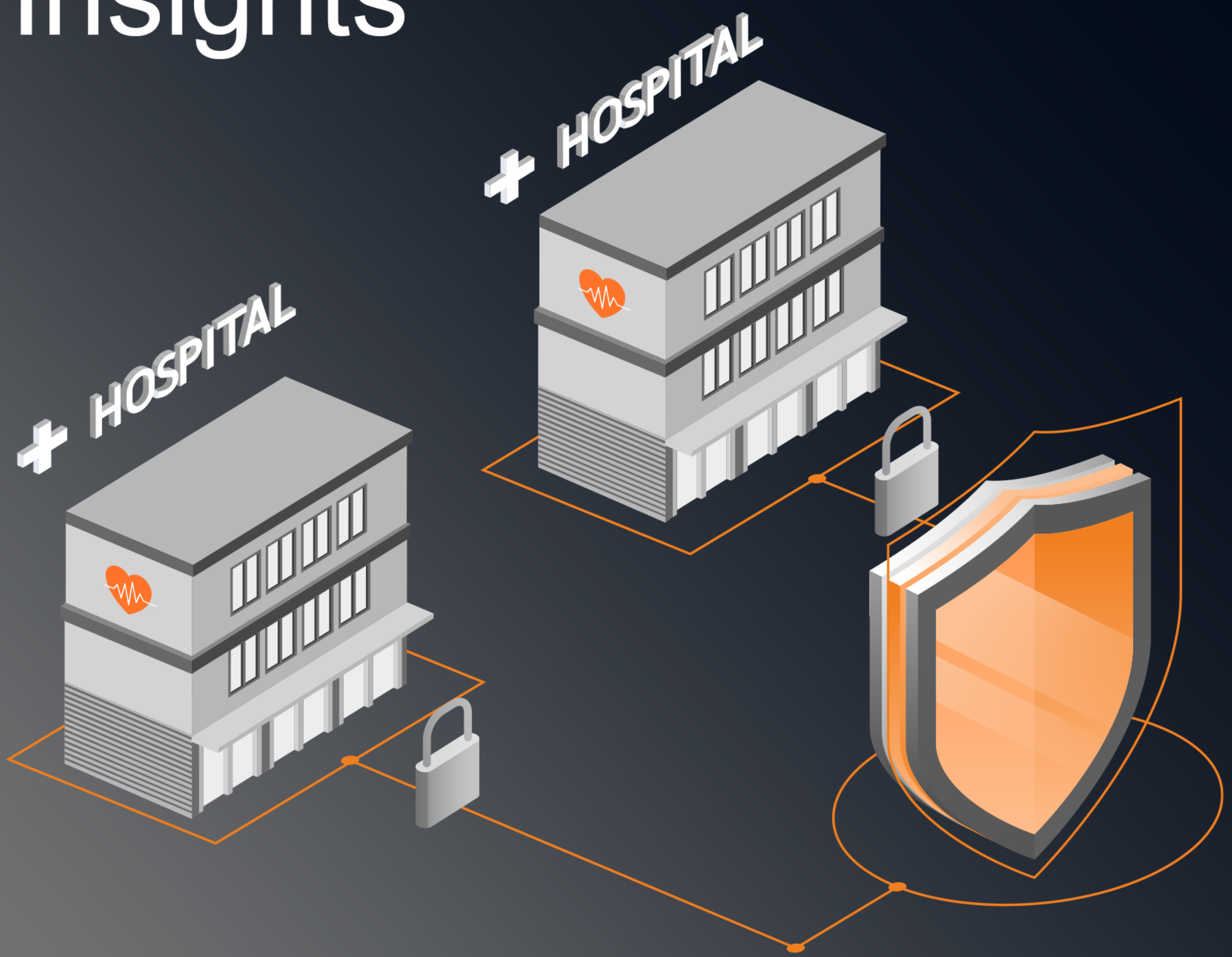
enclaive

Translate Patient Records into data-driven Insights



www.enclaive.io

Confidential Containers in Action: Securing Patient Records in a GDPR Compliant Way

Healthcare is one of the most important and impactful areas in our society, with access to patients' most private data: their medical records. Healthcare institutions share a unique position when it comes to protecting data, as they are responsible for safeguarding their patients' highly sensitive and discrete data.

Because of negative consequences, such as financial and reputational costs, resulting from data breaches, medical institutions are extremely hesitant to share or allow access to their sensitive patient data. Therefore, a move to the cloud without jeopardizing data security and privacy seemed far stretched, until now.

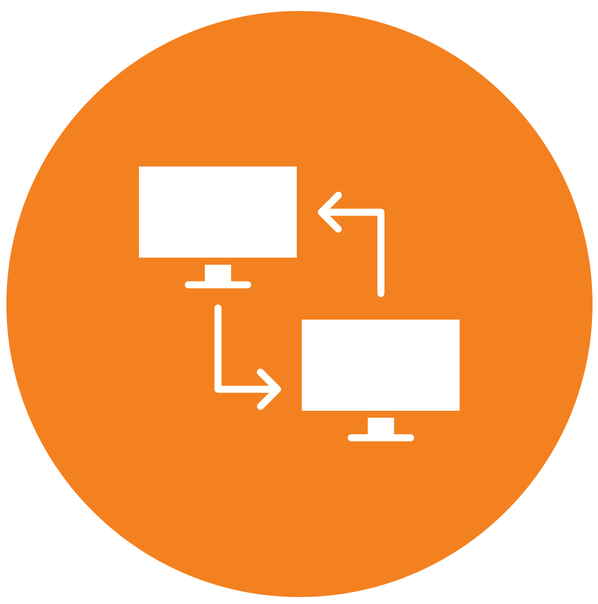
ENCLAIVE GMBH
WWW.ENCLAIVE.IO
CHAUSSE ESTR. 40
101 15 BERLIN

The Challenges

Two primary challenges healthcare and medical research institutions face are the need to **exchange data to improve patient care and reduce cost** and insights on the one hand, and the legal and ethical obligation to **prevent data breaches** on the other one.
Enabling data exchange is a key driver for holistic patient care and medical breakthrough. Any such development requires sufficient high-quality data for sharing initiatives.

But the primary impediment to accessing more datasets was the **increase in data privacy regulations like GDPR** within the healthcare sector. In some countries, hospitals, clinics and medical institutions are considered critical infrastructures and are forced to implement a plethora of methods to protect against any form of data privacy violation. In particular, keeping **data anonymized** at all times, specifically while trying to leverage such data sets in digital form poses a great challenge for healthcare organizations.

How can you keep patient records secure during data exchange?



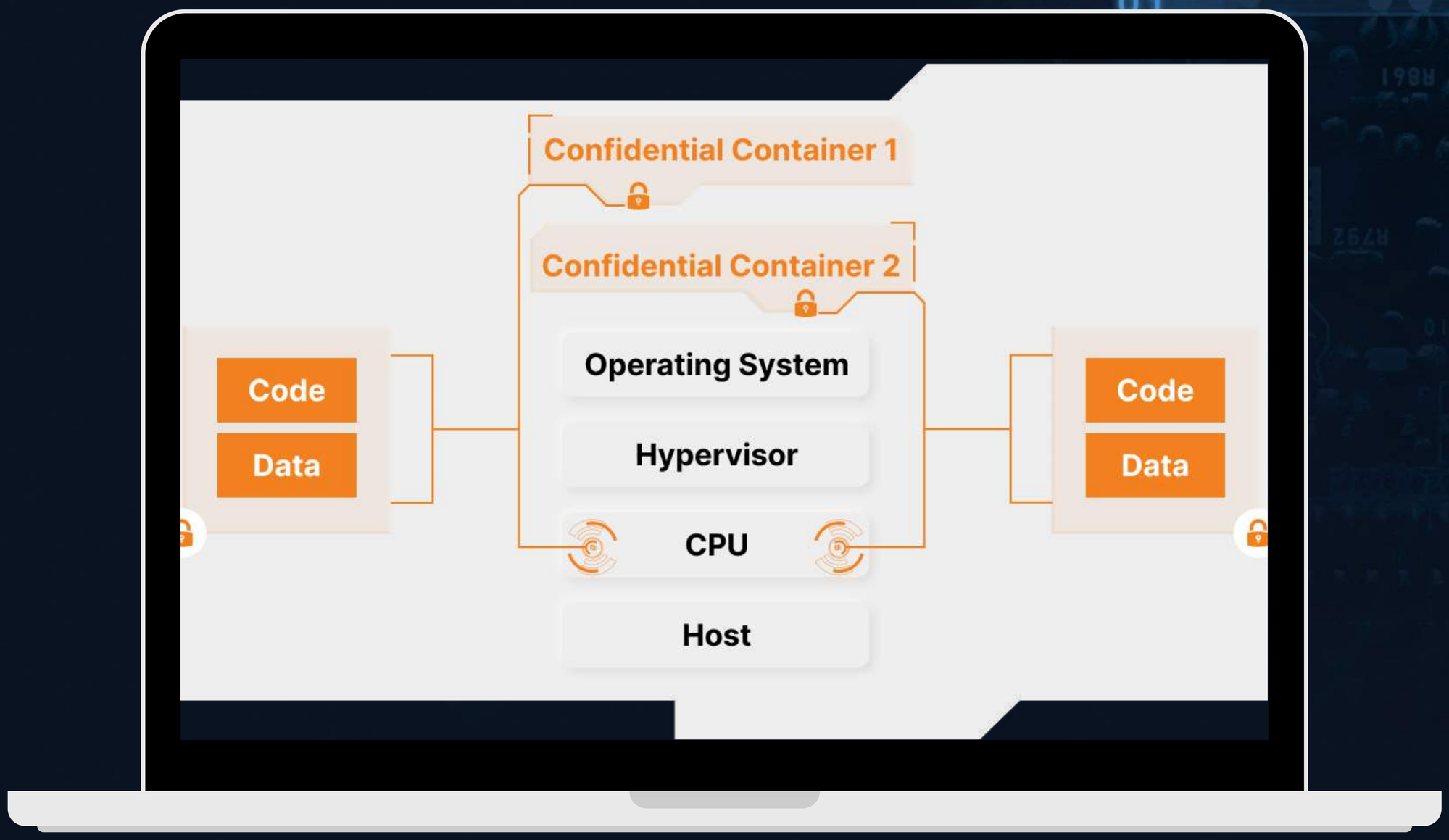
How to prevent data breaches and ensure data privacy compliance?

Solution Overview

In this context, the emerging technology of Confidential Computing can be used to secure patients' medical history and sensitive data, while also complying with data privacy regulations like GDPR.

In a nutshell, Confidential Computing is a new computing paradigm **safeguarding** that patient **data** and sensitive data at **any moment in time** and **anywhere** while it is **stored, looked up, edited or processed remains encrypted and shielded against data breaches**. Only authenticated users may access the data.

By design, **patient data is given the safest harbour**. Healthcare software companies can turn their applications into confidential applications with ease thanks to enclaive's revolutionary confidential container technology.



Patient records secure and privacy compliant anywhere while in use - Digitalize IT with Confidence

Enclaive' Confidential Containers leverage the Confidential Compute Technology and are designed to protect both the data and the application, an any - even untrusted - infrastructure. Throughout the data lifetime, **sensitive data is always encrypted in memory and stays protected while being processed.** Confidential computing technology ensures that patients' data stays anonymized, while - say patients' health care plan is being created and tracked by different medical care centers.

Enclaive reduces the **legal and IT-compliance** efforts by providing Confidential Container technology that support **GDPR regulations** at all times. Hence, any attempt to hack this information is prevented by the privacy box, allowing for storing and processing of healthcare data in a privacy-enhanced way. Moreover, the container may be **attested** at any point in time to the integrity and confidentiality of the code and data, easing the obligation to document proof.

What our customers say:

> **"In the transition of digitalizing the hospital IT (KHGZ) enclaive's technology helped us to implement many new IT projects with ease and in consensus with the data security officer."**
> **Alexander Mommert, CEO Immanuel Klinik Rüdersdorf**

Sharing Data without Sharing - Easy multi-party Collaboration in Medical Research

Such confidential microservices would also enable secure multi-party data sharing for different purposes. For example, multiple hospitals can combine their data to train AI for detecting diseases, say, given pictures from CT scans. Exchanging data for research purposes would not come at the detriment of data privacy, though. Working within enclaive’s Confidential Containers ensures that patients’ data remains confidential during each step of the process. This way, the patient's privacy is protected and hospitals or other data owners (i.e. research institutions) remain in control of their valuable data.

Therefore, by using Confidential Computing technology, healthcare providers and medical research institutions will be able to join hands globally and work seamlessly with sensitive data, without having to worry about data security breaches at one or the other end. With the seamless and scalable data security that is required by the complex workloads associated in clinical settings.
With a secure infrastructure in place and by using real-time auditability, the healthcare organizations can now benefit from the data security necessary to reduce the development time of new AI solutions, improve the clinical outcomes for patients through multi-party collaborations and therefore, hopefully, realize new medical breakthroughs.

Read enough? Click here to jump right in.

Why should you choose enclaive?

Give healthcare IT the safest place

Make Data Privacy a friend - not foe

Frictionless deployment

Be ready for Compliance Audits

Testimonials:

> **"Our fintech platform for the eHealth sector requires the highest security and privacy compliance, which we could implement at reduced costs with enclaive technology."**
> **Martin Buhl, CEO cure digital finance GmbH**

> **"In view of the enormous challenges, we are facing worldwide in the clinical and care context, it is obvious that sustainable solutions require interdisciplinary collaboration between academia, politics, industry, and civil society that are build on data protection at the highest possible levels. Leveraging Confidential Computing is a key enabler for innovation and transformation in Health Care."**
> **Ljubisav Matejevic, President & Founder The Global Clinical & Care Coordination Forum**

Why should you choose enclaive?

Give healthcare IT the safest place

Wrapping healthcare IT with confidential containers means deploying the highest standard of security and privacy to protect sensitive data. It is so secure, that even the underlying infrastructure administrator may not access it.

Make Data Privacy a friend - not foe

By design, data while in use is fully encrypted. Only legitimate endpoints may access the data in cleartext. This way, Confidential Compute is a modern data anonymization technique, as no clear text data may be leaked.

Be ready for Compliance Audits

How can you prove that you have taken the best efforts to protect your IT? Running your IT shielded by confidential containers allows you to audit the containers and obtain a digital certificate that sensitive data runs in confidential containers.

Frictionless deployment

Our highly secure containers are built to work right out of the box. No changes to the application code or SDKs are required.

Want to know more?

Get in touch and let us walk you through a demonstration of how our Confidential Containers can secure patient records while also accelerating AI development within your company.

>>> Watch a demo

>>> Try it out

If you want to get to know Enclaive:

>>> Product Portfolio

>>> In the Press

>>> About Us

EMAIL:
contact@enclaive.io

WEB:
enclaive.io