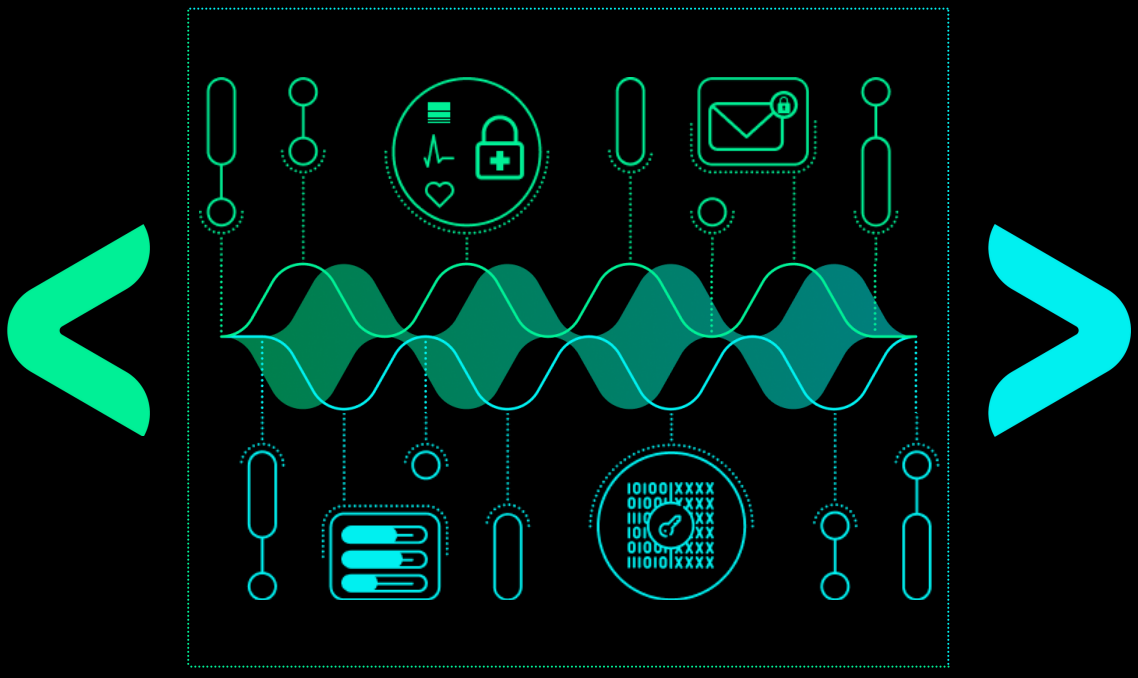
CRUD Encryption

Protect The Sharing Of Sensitive Data In Healthcare



Author
Mia-Care Team

The concern of sensitive data management and protection in healthcare has always raised interest among experts, creating some disputes over time. The imposition of rules for **guaranteeing the confidentiality of personal information** often clashes with the urgent need for doctors to act quickly for the wellbeing of patients. Furthermore, dealing with a bureaucratic system keen to create inefficiencies raises the level of complexity.

It's just with the definition and diffusion of General Data Protection Regulations (GDPR), which occurred in 2016, that **data security and privacy in the European Union changed radically.** In this perimeter, health providers and hospitals gradually started to give real importance to the level of confidentiality destined for patients.

Even though the GDPR doesn't have a specific section dedicated to clinic data management, these clusters of information are classified as sensitive data and include:

"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."

(Art. 4, n. 15 - GDPR).

With the diffusion of digital technologies worldwide enhancing the sharing of high volumes of sensitive data, article 35 of GDPR legislation requires companies to carry out an impact assessment (or DPIA - Data Protection Impact Assessment). This process aims to **identify and mitigate the risks** arising from the mistaken use of new technologies in processing personal data.

Following the directives promoted by GDPR general structure for risk management, among healthcare companies emerged the need to **define shared best practices** for assessing the impact of new technologies when personal clinical data are involved. In this context, a good source of value can be found in the Health Technology Assessment (HTA) model, which includes the requirements defined by the GDPR within a multidisciplinary approach. Thus, in addition to privacy and data protection, it is monitored **how new technologies condition care pathways and the efficacy of medical treatments.**

This method helps to estimate how digital technology directly conditions the company organization, the business processes, and the adoption of new therapeutic practices, by overtaking the distance between the IT function and other departments of the company. The evaluation includes the following aspects:

- Analysis of the health problem and characteristics of the digital solution;
- Safety, not only from a technological point of view but also from a health and organizational point of view;
- Clinical efficacy;
- Personal data protection;
- Patient Perspective;
- Economic aspects;
- Organizational aspects, and integration of data and processes;
- Socio-cultural, ethical and legal aspects.

What is CRUD Encryption, and how it contributes to sensitive data protection?

Mia-Platform is very careful in listening to feedback from clients for enriching the product with new features that have strong market traction. Among the most discussed requests, two, in particular, stand out: the protection of databases from unauthorized access and the **blurring of specific clusters of information to people with no permission.**

For this reason, Mia-Platform v8.0 successfully introduced a new component of CRUD service, allowing the management of privacy and sensitive information as described above. How? Working on confidentiality levels and visibility of data gathered within the systems of record.

The **CRUD Encryption** can be activated on one or more document fields and execute the data encryption of selected data before sending them to databases, blocking the visibility to users' profiles that do not have the grants to access.

The information flow that processes data is simple and can be carried out in writing (data encryption) and reading (data decryption).

It is worth paying attention to the value of the encryption keys in the encryption process, as their loss would make it impossible to access previously saved data. In fact, in order to properly execute the activity, two elements are needed:

- The **Master Key** used to encrypt the various decryption keys;
- **Data Encryption keys**, generated to perform the data encryption/decryption action and saved in a collection created on the database.

The valuable use of the new functionality in the healthcare sector: the experience from Mia-Care

Mia-Care was born as a Mia-Platform vertical for healthcare providers and received remarkable attention and acknowledgments from the market as one of the most innovative technology providers.

The Mia-Care team has to deal every day with requests related to a **punctual and secure way to manage sensitive information.** From the anagraphic, walking through the identification of chronic or acute diseases, to the invoicing process, the use of CRUD Encryption has strategic importance in current projects.

In this perimeter, the European GDPR suggests the best practices to manage data for a dual objective: on one side, to protect the level of sensitivity on information shared, on the other side, to face the risk of data breaches.
In particular, it is interesting the distinction between **anonymization and pseudonymization of data.** While pseudonymized information can be retrieved using a decryption key, data anonymization is an irreversible process.

To better understand the benefits granted by CRUD Encryption, it is relevant to consider a practical example.

Within a project that enables the provision of health care services to private citizens, the use of the decryption function of CRUD service helped to define the different levels of data sensitivity and **decide whether to encrypt or decrypt information, depending on who needs to use it.** This functionality also allows the activation of pseudonymization, disconnecting the health insight from personal data.

Therefore, if the doctor requests to view the patient's health history, the information will be clear. However, if the administrative function needs data such as the anagraphic, the clinical information (for instance, the pathology or the therapy) will be hidden.

To work efficiently on users and authorizations, the CRUD Encryption interacts with ACL Service (Access-control List) to provide different visibility grades depending on the users' role. This microservice applies access control rules to a set of data on two dimensions: by row, for viewing only the documents created by the user; by column, limiting the fields that a user can see, based on the profile granted.

To conclude, decryption keys are decentralized and are managed by the Key Manager that operates as described before, ensuring the highest level of security. If an external entity forces access to the company's databases, it would not be possible to relate the personal information of the beneficiaries with medical history documents or medical reports.

Do you want to deep-dive into the technicality of described microservices?

- CRUD Encryption;
- ACL Service.

Do you already know Mia-Care?

Mia-Care software suite contains unique capabilities and resources to seamlessly design, build, deliver, and orchestrate digital service for every type of digital platform leveraging a modern web architecture based on fast data, process automation, containerization, and advanced analytics. Our Platform is state of the art compliant with security and privacy regulations both for EU and US applications and it is designed to allow easy integration with PA/EHR infrastructures. Learn more at www.mia-care.io