Open Source foundation of a Trust Network based EHR

Antoine Duchâteau, Taktik sa

ORTHANC CON 2019

GNUHealth CON 2019

iCure platform

A common foundation for Electronic Health Record

iCure is not a standalone EHR, it is not a HMIS.

iCure is an open source platform for software EHR and HMIS developers

It is a ground layer upon which you build medical software

Its goal is to ease the creation of innovative medical software that **share data**

Why a platform ?

- Spur innovation on the constrained belgian market
- Healthcare data must be shared to reduce Social Security costs
- Healthcare data should not be shared due to privacy concerns
- EHR development costs explode
- Data Model is not consistent
- Sharing data is too complicated

Open Source foundation of a **Trust** Network based EHR

It is all about trust

TRUSTED

Replicates a peer 2 peer network of trusting actors.

Trust is transferred by sharing cryptographic keys

ENCRYPTED

Encrypted on HCP computer

Stored encrypted in the cloud

AVAILABLE

Multiple replicas

Multi clouds solution

Local version of the data

TRANSPARENT

Open source

Externally auditable

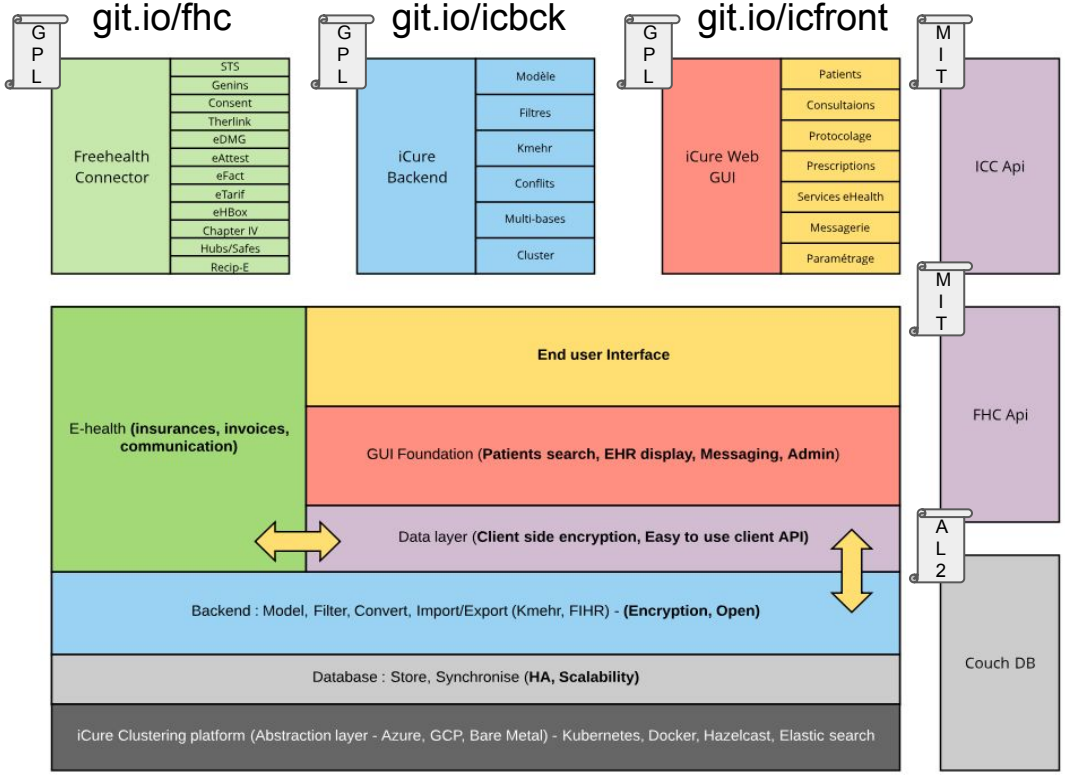
PATIENT-CENTRIC

Combines data from multiple HCPs..

Virtual care group around each patient.

Finely grained cryptographic data access control

What do you need to make an EHR



What people are doing with it ?

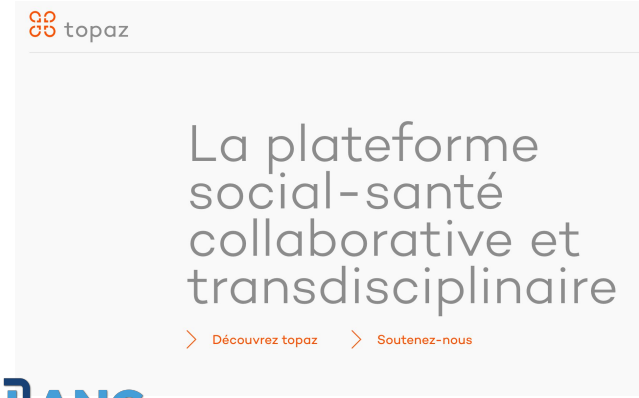
- Two Software Companies
- Build a full multi-disciplinary, problem oriented web based EHR
- Medispring & Topaz
- 18 months development (team of 5 developers)
- 22 certifications

Medispring

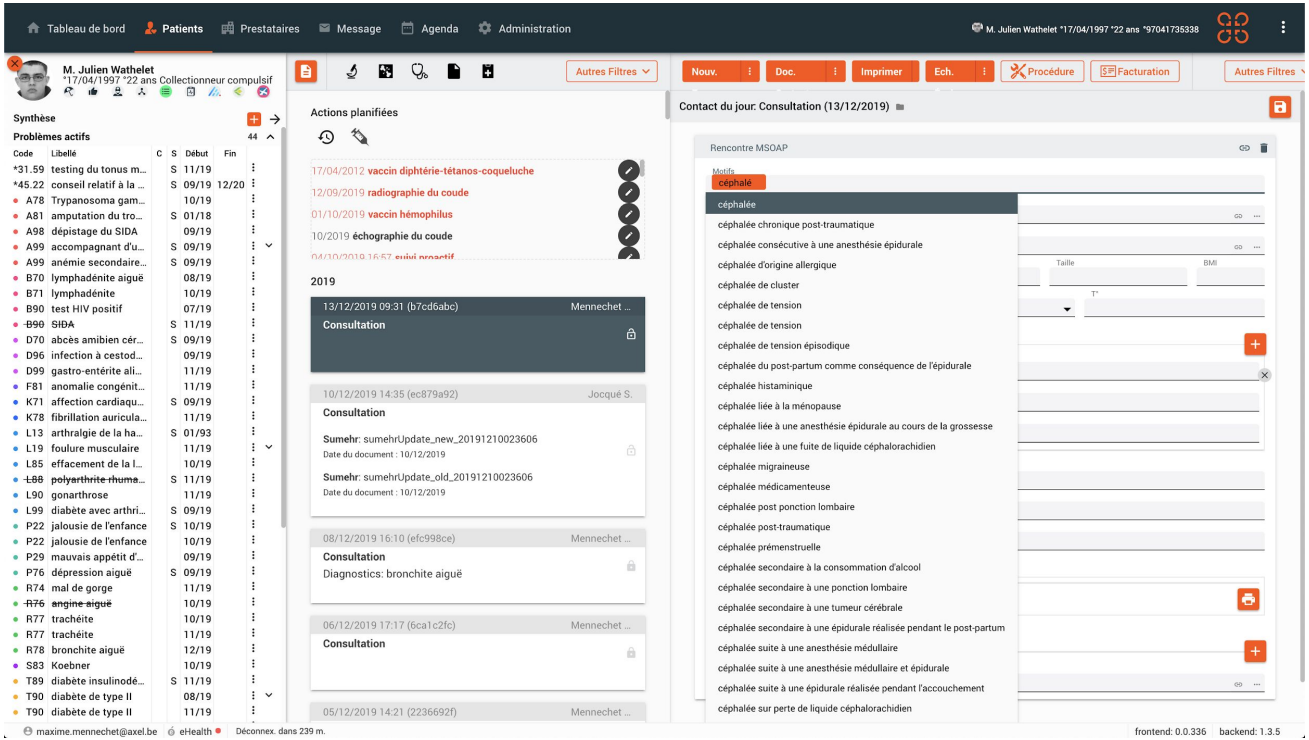
- Co-operative model
- Closed source
- 1500 Doctors

Topaz

- Social Medicine
- Open source
- 800 Doctors, nurses, physiotherapists



Topaz



ORTHANC CON 2019

GNUHealth CON 2019

Thank you!

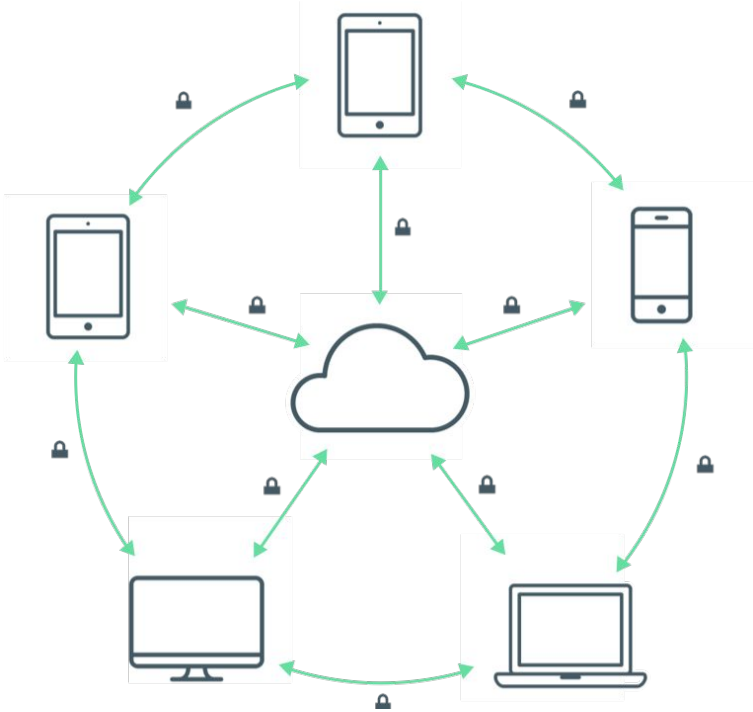
TAKTIK
Avenue Reine Astrid 92
1310 La Hulpe
+32 2 333 58 40
ad@taktik.com

Built on trust

Trust is at the core of the patient-doctor relationship. When a patient sees a doctor for the first time he initiates the creation a web of trust that will eventually connect all the healthcare professionals responsible for his health.

Each time a healthcare professional refers a patient to a colleague this person transfers this trust by sharing the patient's medical with another doctor.

iCure replicates this structure by sharing the patient's health records on a peer-to-peer basis.



Built on trust

iCure manages this web of trust by managing the peer-to-peer connections between healthcare professionals. Each referral becomes an explicit data node in the database.

Medical data is shared among healthcare parties using the encrypted document master keys for the doctor the patient is referred to.

Rules can be created to automatically share (specific) data with designated healthcare professionals.

These access restrictions cannot be circumvented, as they are enforced through cryptography.

Secure & encrypted

iCure aims at centralising the medical data of a whole population in the cloud so that data can be shared seamlessly between healthcare professionals.

The consequences of a breach, or misuse of personal data, could be disastrous for the privacy of the exposed population.

iCure mitigates these risks by ensuring that the healthcare professionals never have to trust third-parties with their data. The medical data is anonymised and encrypted on the computer as it is being typed. iCure does this through a keys system that prevents anyone but the original author to decrypt it.

Data sharing relies on the same encryption scheme and guarantees that only the recipient of a piece of information can access it.

Secure & encrypted

Public key/private key encryption is central in iCure's data model. Each healthcare professional has a personal AES master key protected by his own private RSA key.

The AES master key secures the foreign keys used to link a piece of medical information to a patient. The AES master key is also used to encrypt the medical data itself.

When a healthcare professional wants to share data with a colleague, he creates an AES share key and encrypts it with the RSA public key of his colleague. He then uses that AES share key to secure the foreign keys and the medical data he wishes to share.

Available

Electronic Health Records must be available no matter the circumstances. At work or on the road, with or without internet access, a healthcare professional must have access to its data.

iCure was built with peer-to-peer synchronisation in mind. Any two members of the same team can synchronise their records; just by being on the same network.

The cloud acts as a central hub where anyone can get the most up-to-date data.

This ensures patients and doctors that their data is always available and can be used to improve patient care.

Available

iCure guarantees availability by relying on the rock solid offline/online synchronisation capabilities of CouchDB. Each user always has a copy of his database stored locally.

https://bit.ly/2He7QQU

The whole data model has been designed to allow for easy and automatic conflicts resolution.

Whenever conflicts arise, the data model allows for a combination of the available data on conflicting branches. Healthcare professional can fix or remove duplicate data when using their EHR.

Transparent & open source

iCure's micro-services and iCure's reference web GUI are both open source. This guarantees that no collection of data can be performed alongside the standard secured/encrypted data persistence.

This also ensures that the iCure platform can be adapted by the software vendors that rely on it.

The OpenDMI alliance brings together 3 belgian software editors and dictates the overall evolution of the platform in terms of data model extensions and standardisation of the codification.

The OpenDMI alliance is open to any software vendor that wishes to build its solution on the iCure platform.

Transparent & open source

The full iCure stack is available on github.

https://git.io/fhc
https://git.io/vpL0S

We accept pull requests from any vendor that wishes to contribute and propose a professional support program.

The support programs guarantee response time for technical issues that could arise while using the iCure platform.

It also guarantees that possible changes to the models are submitted during OpenDMI meetings for approbation and inclusion.

Patient-centric

EHR editors create EHR software centered around their direct customers : doctors, nurses, physiotherapist…. Independent partial data sets are created by each HCP for their patients.

The iCure platform is patient-centric. It combines information coming from multiple healthcare professionals in one single shared dataset, creating a virtual care group around each patient.

iCure's finely grained cryptographic data access allows healthcare professional to control what information is available to their colleagues and what information stays private to him alone.

Patient-centric

iCure Cloud combines data coming from a series of distinct CouchDB databases belonging to different users in one unified dataset.

Data created by a doctor is stored in their database. The cloud application server queries the databases of all the doctors connected to a patient - and others who have shared information with him- to provide a unified view of the distributed dataset.

Each document (patient, contact, health element) requires a master key to access its content. These master keys are encrypted and can only be decrypted by the authorized healthcare professionals who own the necessary decryption keys.