Association Française des Hébergeurs Agréés de Données de Santé à caractère personnel

FRENCH APPROVED EHR HOSTING

ISP Connect – June 8th, 2017

Requirements for EHR hosting

- Prior approval by the national DPA and the Ministry of Health.
- Requirements
  - Legal : patient approval, description of application and hosting conditions, patient access to logs
  - Organizational / Ethical : Implementation of an ISMS, hiring of a doctor in medicine
  - Technical : dedicated infrastructure, two factors authentication, encryption, logs of every access to patient data
  - Financial : reasonable guarantees of business continuity
- The hosting provider manages security risks for the whole processing chain, from the end user to the stored data.

Origin and rationale

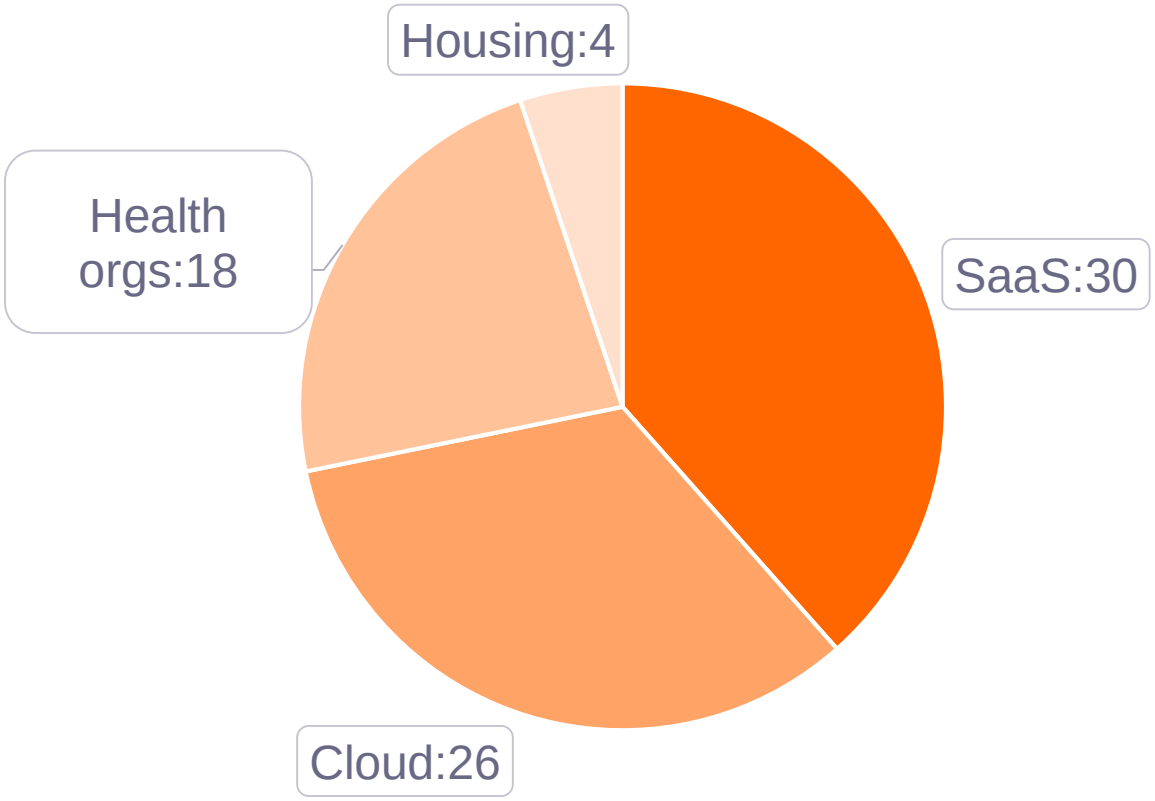
- Studies by the DPA in the early 2000's
- Patient protection law of 2002
- Strongly influenced by the project of a national EHR repository.
- First approvals delivered in 2010

Thus :

- Probably a total misunderstanding of the generally accepted role of an hosting provider
- Yet extremely effective in bringing expert support on data security to a number of immature players

Players

78 approved structures today



Hosting and application

- Approval was originally designed with a lot of confusion between application and hosting.
- Authentication, authorizations, traceability are in the scope of the approval.
- The hosting provider has to assert the compliance of the hosted application.
- For cloud providers, it is most often addressed through requirements in the hosting contract.
- The approval is bound to the contract template.

Drawbacks and benefits

- Approval is a long and uncertain process
- The hosting company is nailed with the approved solution and contract
- Each application must be checked for compliance

- The number of potential applications is huge
- The approved companies are highly visible
- The knowledge of the intricate rules and regulations regarding health data and applications is valuable
- Even applications that are not legally constrained to use a approved hosting look for the brand

The association

- AFHADS was created by the first approved structures in 2010.
- It gathers half of the structures around the idea that approved hosting is not a mere label upon hosting, but a totally new role with a social impact.
- It has gained recognition of French authorities and participates actively in the definition of the national security policy for health data, including legally opposable requirements.
- It has fought actively for the last two years to preserve the mission of its members … and failed.

The end of the game ?

In 2018 the approval will be replaced by a certification.

Pros :

- Fair and explicit process
- Accountability allows for flexibility in offers
- Based upon ISO 27001, brings recognition out of France

Cons :

- The application specific features have been removed from the scope of certification
- General purpose hosting companies can enter the game
- The brand will not bring any more specific value

How we intend to react

- The association attempts to create a label of its own on top of the certification.
- It would reintroduce the assistance in asserting the compliance of the applications.
- The demand can be carried by :
  - The recognition of the service brought in the existing frame
  - The fear of GDPR, where approved hosting companies can bring their knowledge of risk analysis and mitigation.
- It could be generalized at the European level, typically within a GDPR code of conduct.