Nextcloud

Industry Analysis, 2018

Where should healthcare data be stored?

According to the Information Commissioner's Office in the UK, healthcare data breaches accounted for 40 % of late 2016 security incidents[1]. This type of information is a special nightmare to deal with. On the one hand, the data is obviously highly sensitive, on the other hand, accessing up-to-date medical data without delay can be a matter of life and death for patients.

What you should think about before picking a solution:

- Can you track or limit the sharing or downloading of specific files if you need to for compliance requirements?
- Can you change or adapt the whole process if new laws come into force?
- Can you at least migrate part of all of your data out of the cloud to another place if you need to, or is it too costly?

The tidal wave of digitization now raises security issues. Benefits are manifest: medical information can be transmitted easily from one organization to another, patients can have better access to their medical records. But it raises questions: **where and how to store the information properly and securely?** Each organization which needs access to the data has different governance, management and rules, and it is hard to implement consistent data security policies and training to educate staff on keeping data safe with all the different requirements. Cédric Cartau, Chief Information Security Officer at Nantes University Hospital notes[2]:

> "In the next 5 to 10 years, we can expect far more security issues, which will require bigger budgets, more staff and teaching best practices."

And what do you do if you are confident in your security policy but you know that this or that hospital you have to share with is not as sophisticated with regards to digital hygiene? Consistent governance is hard: the mix of private and public organizations in most countries like the UK, France, Germany and the US makes unified protocols and policies difficult.

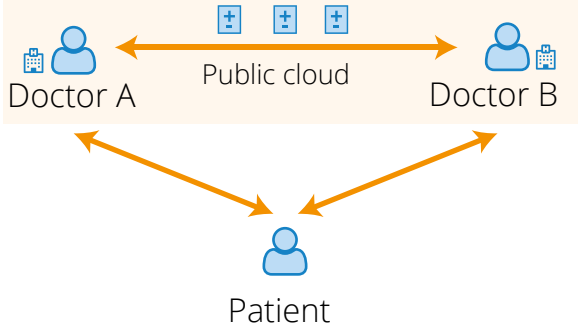
Expensive chaos

Today, the situation is chaotic at best with PBS asking if health care hacking has become an epidemic[3]. Healthcare data can leak from everywhere: **according to this report[4] from the U.S. Department of Health and Human Services, the health care industry has averaged close to four data breaches per week in 2016**. Patients also carry these vulnerabilities with them, in the form of minimally secured smartphone health apps. And this data is worth a lot of money!

Nextcloud

"Electronic health records are 100 times more valuable than stolen credit cards",

said James Scott[5], co-founder and senior fellow at the Institute for Critical Infrastructure Technology (ICIT) in Washington D. C.



Risks of public clouds:

- Ransomware
- Hacking
- DDOS attacks
- Loss of compliance
- Vendor lock-in

Public clouds: no solution

IT teams do not have a substantial budget dedicated to security concerns. And when you are attacked every seven seconds on average like the Beth Israel Deaconess Hospital[6] you have a real problem. **Some health care organizations made a surprising move: put their data into the public cloud**. In terms of security, it is indeed a better alternative than building your own system on a shoestring budget. Microsoft, Google and Dropbox spend millions on security. Their teams patch security issues quick and their core business is making data accessible whenever and wherever it's needed.

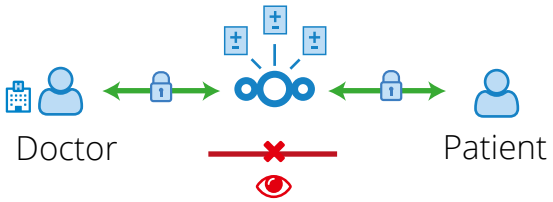
But public clouds are not set up very well for handling healthcare data. First of all, using public clouds raises privacy concerns, which is particularly worrying when it comes to dealing with such sensitive data. Second, public clouds don't really solve the security issues! Due to the typical consumer-focused nature of public clouds, IT teams have to rely on third-party tools to ensure that only the right people have access to medical data and to enforce the secure use of those clouds. These tools for example provide Identity as a Service (IaaS) and help manage staff-owned devices and sharing. But this is only moving the problem. **Using several tools layered on each other multiplies complexity and increases the opportunities for costly mistakes as well as the surface of attack**. Now, a breach on several levels and in a variety of tools can leak data!

Last but not least, transparency, crucial for compliance, is often lacking. When a data breach takes place, laws in many countries demand that the people whose data might have been compromised get notified; and that law enforcement is informed so they can take action. But the cloud application providers have built up a questionable reputation for keeping breaches hidden for years – **making it impossible to be 100 % certain if and when data was stolen.**

Private cloud: stay in control

Nextcloud features a built in DICOM viewer with patient data handling

The most powerful and elegant solution to the security-vs-accessibility problem faced by the medical sector is implementing a private cloud solution. The existing data storage and access technologies, and more importantly, existing governance processes and tools, can be leveraged by software like Nextcloud, making the data caretaker's need available easily and quickly while IT can stay in control.



Doctors and patients can easily exchange sensitive medical data using a secure private cloud solution like Nextcloud.

Nextcloud Files offers a powerful, easy to use file sync and share solution. It gives medical professionals access to their files through an intuitive **web interface, easy mobile applications and a desktop sync app** which keeps files in one or more folders always up to date. This versatility makes Nextcloud a great fit in a market trend for **Telemedicine, remote and Mobile Health care.**

The flexible nature of Nextcloud enables **deep integration in existing infrastructure**. By keeping data where it currently is, investment in IT infrastructure like file storage, industry-specific and in-house applications is protected, making Nextcloud a **cost-effective solution**. This is strengthened by the ease of deployment and maintenance, giving Nextcloud a strong TCO advantage over competing products.

Nextcloud is designed with an extensible, open source core and standards-based **Application Programming Interfaces (API's)** which can be quickly adapted to deal with specific use cases like E-Patient files (digital patient dossiers) and can be integrated in a variety of other applications.

Any IT team working to support health care professionals struggles with the complexities of providing large amounts of data in a quick, easy but highly secure way. Nextcloud provides a **uniquely fitting solution for this market**.

Nextcloud

Powerful File Access Control capabilities enable administrators to control, optimize and secure data flows through their cloud technology.

Encryption of data on storage allows medical organizations to optimize costs by taking advantage of public cloud storage while securing the data with encryption, keeping encryption keys on-premise.

Ability to **restrict and monitor access to data** to a specific group of users and to set an expiration date when sharing files is a real need for medical organizations.

Developed with **verified, industry-leading security standards** and offering unique tools to verify the security of private clouds, Nextcloud offers the most secure and cost-effective private cloud solution on the market.

HIPAA:

Nextcloud meets all **Technical Safeguards requirements,** supporting full compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Nextcloud GmbH is committed to ensure its software keeps PHI (Protected Health Information) private and secure. We have implemented features, policies and procedures designed to ensure compliance with Federal and State information security laws, regulations, and rules, and monitor ongoing compliance efforts.

Nextcloud GmbH
Kronenstr. 22A
70173 Stuttgart
Germany

E sales@nextcloud.com
T +49 711 896656-0
F +49 711 896656-10

nextcloud.com

About the author

Fabian Liedtke
Account Manager

Fabian worked for various industries always close to the customer and has been in the IT industry now for several years with a focus on customer relationship management. He is passionate about innovative and new technologies and his primary goal is to help our customers to fulfill their vision.

Sources

[1] ico.org.uk/action-weve-taken/data-security-incident-trends/

[2] digitalforallnow.com/en/what-are-the-implications-of-healthcare-data-security-interview-with-cedric-cartau/#!

[3] pbs.org/newshour/science/has-health-care-hacking-become-an-epidemic

[4] ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[5] information-age.com/can-cloud-save-nhs-data-breach-epidemic-123465121/

[6] spectrum.ieee.org/the-human-os/biomedical/devices/5-major-hospital-hacks-horror-stories-from-the-cyber-security-frontlines