Local storage

or

Cloud hosting

Michel ARNOULT
2017/may

kayentis
Dedicated to eCOA & Patient Engagement

Michel ARNOULT, Consultant in Data Collection
and Data Management in Clinical Research in

Contents

Introduction

Over the last 25 years the collection of clinical research data has moved from paper-based systems to electronic data capture using various tools (e.g. personal computers, tablet devices, smartphones) and made possible by the internet.

In parallel, in the context of a global reach, pharmaceutical companies have relied increasingly on specialist contractors (e.g. CROs, CMOs, data management platforms) to conduct these activities on their behalf.

The widespread nature of high-speed network connections (e.g. ADSL, fibre-optic) has allowed internet-based tools to become commonplace (e.g. Web, electronic mail, IP telephony). Terms such as 'Web 2.0' and 'Cloud Computing' have increasingly entered day-to-day language.

1. What is 'Cloud Computing'?

'Cloud Computing' is a term that is increasingly used to graphically describe the internet.

It allows users to access service, software, and other IT services at distance and to use them via the internet.

Access to the 'Cloud' can be free or fee-paying, public or private.

- **'CLOUD' SERVICES INCLUDE:**

  - Software as a Service (SaaS)
    - Ready-to-use software applications that are designed to meet the needs of regular users or professionals.

  - Platform as a Service (PaaS)
    - Development platforms on which programmers can build and test new applications.

  - Infrastructure as a Service (IaaS)
    - Basic IT resources providing capacity for data processing and storage.

- **THE DIFFERENT TYPES OF 'CLOUD' INCLUDE:**

  - 'Private Cloud': services created and set up for the exclusive use of a single organisation, which can be managed and hosted internally or by a third party.

  - 'Public cloud': open services that can be free or fee-paying and available to anyone who accepts the terms and conditions of use.

  - 'Community cloud': services created and set up specifically for groups of organisations that have common IT needs.

  - 'Hybrid cloud': a cross between the 'Public Cloud' and the 'Private Cloud'. Companies can use the 'Private Cloud' for important or confidential tasks, and use the 'Public Cloud' for tasks that require scalability of resource (e.g. a temporary need for greater processing power).

- **THEORETICAL ADVANTAGES OF THE 'CLOUD':**
  - o Flexibility and the ability to evolve over time (e.g. processing power, storage on demand).
  - o Performance.
  - o Reliability.
  - o Reduced costs in terms of infrastructure and IT resource due to the pooling and sharing of services.
  - o Investments are made by the cloud service supplier, with the client only paying a subscription charge.

- **DRAWBACKS OF THE 'CLOUD':**
  - o Security is perceived as being lower than hosting using a company server, with an increased perceived risk of cyber-attacks.
  - o The need for a continuous excellent network connection between the user and the server.
  - o Reliance on the 'Cloud' provider and the need for contractually controlled access to services.
  - o Implementation and compliance with regulatory demands and good practices (e.g. European Union (EU) Appendix 11, FDA 21 CFR Part 11, ICH GCP) can be difficult for providers who are not always familiar with such constraints.
  - o Since 'Cloud' services involve many providers (e.g. listed below), who may interact with each other, it is not always straightforward to establish their respective responsibilities:
    - Providers' access to the internet.
    - Telecommunications operators.
    - Data storage and data management servers and providers (Data Center).
    - Service providers who have their applications hosted on the system.
    - Other service and solution providers.
  - o 'Cloud' systems are still susceptible to breaking down, e.g.:
    - Amazon's storage services, 28 February-1 March 2017: 150,000 websites affected globally.
    - Microsoft: https://azure.microsoft.com/fr-fr/status/history/
    - Google Drive, 26 January 2016.

2. The 'Cloud' and specific life science regulations (GxP)

The regulations cited below must be implemented by solution and service providers and the 'regulated' company must be able to demonstrate compliance with these regulations:

- o EU Annex 11 and FDA regulations (CFR) ICH GCP E6.

- o FDA 21 CFR Part 11.
    - Validation.
    - Data integrity.
    - Audit trail.

- o Protection of personal data.

- o Laws and regulations can develop differently in different countries (e.g. EU, USA, Russia, Japan, China) and local and regional specificities need to be taken into account (e.g. GRDP was adopted by the EU in 2016 to be in place by 25 May 2018).

3. Traditional 'in-house' hosting compared to the 'Cloud'

The 'regulated' company must ensure that the IT infrastructure that uses the applications that can have an impact on the health and quality of life of patients is properly controlled and managed (e.g. in terms of investment, training, installation, validation, operation, control, maintenance, change management, quality assurance documentation) and that it conforms to all applicable regulations (e.g. ICH GxP and its local specificities, adopted by e.g., FDA, EMA, ANSM). In particular, IT systems should be validated to ensure data integrity throughout the various research and production processes of products that are intended for use by patients.

Using a 'Cloud' solution to reduce IT costs and allow the implementation of new technologies outsources the process of data collection, management, and storage. Even though this lessens some IT investment by the 'regulated' company, this does not exonerate it from its responsibilities.

4. Recommendations

The 'regulated' company's team with the responsibility of choosing the 'Cloud' services provider and of implementing the contract should consider several factors (experience, quality assurance, IT, regulations, legal, data privacy).

The choice of a 'Cloud' solution means that the 'regulated' company will need to modify its management of various controls and its solution provider supervision, while at the same time maintaining overall responsibility for data integrity and compliance.

The 'regulated' company must continue to apply the same best practices for the selection of service providers and for their qualification as fit for purpose (by audit).

- It must, additionally, have knowledge of the localisation of the hosting for the 'Cloud' (EU countries have an agreement for the protection of personal data, e.g. 'Privacy Shield').

- It must know if the 'Cloud' provider itself uses subcontractors for 'Cloud' hosting (e.g. Amazon Web Services, Microsoft Azure, approved hosting sites for clinical data in France).

- The provider must guarantee a quality of service (Service Level Agreement) available 24/7 in terms of:

  o Data back-up.

  o Rescue plan.

  o Metrics available to the client.

  o Reversibility conditions at the end of the service provision must be documented in the contract.

Providers of 'Cloud' services (GxP qualified Cloud) to companies in the life science sector (Pharmaceuticals, Biotechs, Medical Devices) must take regulatory demands into account and adapt their quality systems (QMS) accordingly to allow client and regulatory authority audit.

Companies whose solutions and services are intended for the pharmaceutical sector have started such steps towards compliance, and offer 'hybrid' solutions that include quality control platforms and are qualified to be audited or inspected.

Another approach is based on using specialist providers who are certified in hosting personal health data (according to French government policy detailed in the Journal officiel de la République Française, 13 January 2017).

References

[1] "The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology" by Peter Mell, Timothy Grance, NIST Special Publication 800-145, September 2011

[2] "Challenges for Regulated Life Sciences Companies within the IaaS Cloud" By Robert Streit and Anders Vidstrup, Pharmaceutical Engineering, September/October 2014

[3] "Validation of Applications in a Cloud" by Ivan Soto, IVT Network, April 2015

[4] "A Survey on Data Integrity Techniques in Cloud Computing" by Mahesh S.Giri, Bhupesh Gaur, Deepak Tomar, International Journal of Computer Applications, Volume 122 – N°2, July 2015

[5] "Building Trust in a Cloudy Sky – The state of cloud adoption and security", Report by Intel Security, September 2016

[6] "Why Cloud: The Buyer's Guide to Cloud Security" E-book by Akamai

[7] JO de la République Française "Ordonnance N°2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel" https://www.legifrance.gouv.fr/eli/ordonnance/2017/1/12/AFSZ1626575R/jo/texte

kayentis

Dedicated to eCOA & Patient Engagement