From: OC GCP Questions
To: [redacted]
Cc: [redacted]
Subject: RE: Cloud storage
Date: Friday, September 16, 2016 1:30:00 PM
Attachments: [redacted]

Dear [redacted] -

Thank you for your question and your patience in our response. We consulted others within FDA about your question, and here is the response they provided:

> It is the responsibility of the sponsor or CRO (if the sponsor transfers obligations to a CRO) to assess if the cloud storage system the sponsor or CRO intends to use is secure enough for storing clinical trial data. When cloud computing services are used to store data for FDA-regulated clinical investigations, you should consider whether there are adequate controls in place to ensure the reliability and confidentiality of the data. You should determine if there have been any past security data breaches with the public cloud storage computing services and, if so, that appropriate corrections have taken place. You should consider the following factors (in the bulleted list below) when determining the suitability of the outsourced electronic services. If the outsourced electronic service does not provide the data security safeguards described in the bulleted list, you should consider the risks of using such service (e.g., patient privacy rights, reliability of the data in the clinical investigation and its regulatory implications).
>
> - Validation documentation
> - Ability to generate accurate and complete copies of records
> - Availability and retention of records for FDA inspection for as long as the records are required by applicable regulations
> - Archiving capabilities
> - Access controls and authorization checks for users' actions
> - Secure, computer-generated, time-stamped audit trails of users' actions and changes to data
> - Encryption of data at rest and in transit
> - Electronic signature controls
> - Performance record of the electronic service vendor and the electronic service provided
> - Ability to monitor the electronic service vendor's compliance with electronic service security and the data integrity controls
>
> In addition, it is critical for sponsors or CROs to understand the data flow and know the location of the cloud computing service's hardware in order to conduct a meaningful risk assessment regarding data access, integrity, and security. Data privacy laws may differ from country to country. Therefore, you should perform appropriate risk assessments to ensure that data residing on storage devices outside their country can be retrieved and accessed during FDA inspections.

I hope this information is useful. If you need further information and/or have additional questions, please feel free to contact us at the official GCP mailbox, gcp.questions@fda.hhs.gov. You may also find it useful to access the set of redacted GCP e-mails found at http://www.fda.gov/ScienceResearch/SpecialTopics/RunningClinicalTrials/RepliestoInquiriestoFDAonGoodClinicalPractice/default.htm since we find that many questions and concerns are repeated over time.

Best Regards,

Janet

Janet Donnelly, RAC, CIP
Policy Analyst, Office of Good Clinical Practice
Office of Special Medical Programs, Food and Drug Administration

---

From: [redacted]
Sent: Friday, September 02, 2016 6:22 PM
To: OC GCP Questions

Cc: [redacted]
Subject: re: Cloud storage

Hello FDA Staff,

Please advise if cloud storage systems are secure enough for storing clinical trial data. The publically shared locations of cloud storage we are considering are Google Drive and Drop box.

Thank you for your guidance and assistance. We look forward to hearing from you soon.

[redacted]

[redacted]

[redacted]