Informed Consent Resource Library

Describing Data Across All Technologies

Storage and Archiving Including Cloud, Back-ups and Access

In the consent form and as part of the informed consent process, investigators should inform participants (1) how research data about participants will be stored, (2) the duration of data storage, and (3) what happens to any identifying information. If applicable, describe how research data will be stored and/or with whom data will be shared beyond the end of the study. Your IRB may have a preference as to whether you must explicitly list in the consent the location where data will be stored, such as “in the cloud,” or may use broader language such as “on local servers.” Some IRBs may prefer to emphasize how the data is protected versus specifying storage location. Check with your IRB to understand their preference.

Some investigators use consumer-based cloud storage solutions to remotely store and exchange files with collaborators. Broadly defined, cloud computing refers to third party-hosted computing services that are accessible over the Internet. Popular services include Dropbox and Amazon Cloud, among many others. The cloud can be used for research and provide closed or open access to data.

Most cloud services and apps were not designed with research regulatory compliance or human subject protection ethics or considerations in mind. In many cases, free services offered by cloud providers are not compliant with regulatory requirements such as HIPAA. However, these same providers may have a more secure fee-for-service model that provides adequate coverage. For example, Dropbox can be made HIPAA-compliant within their paid service model and with appropriate changes. It is important for investigators to be familiar with the differences in service tiers for the technology they choose to employ. Check with your institution to inquire about specific pre-approved solutions, or whether there is a process to obtain approval and secure compliance.

Contracting adds additional concerns that make using cloud storage for research data difficult for investigators to navigate. Cloud services ordinarily have non-negotiable end-user license agreements with inflexible terms of use and/or data ownership clauses that may conflict with the research.

IRBs often do not have the expertise to evaluate cloud services, and so IRBs often require sign off from others. An ancillary review should be conducted to determine whether the cloud service is suitable for use in research in light of any regulations like HIPAA and other data privacy laws. If the investigator decides to use a specific cloud service, it should be fully understood and may need to be approved by the IT Department and the IRB for use in research. The investigator should seek IRB, IT, and security expertise to identify and implement appropriate supplemental privacy and security safeguards into the protocol or research project. Remember, users must follow rules dictated by the terms of use. Many institutions own their “own cloud” and do not negotiate for outside third-party services. If, however, a third-party cloud service is offered through your institution or employer, many of the rules may have been negotiated but not necessarily for research purposes. Please be sure to ask.

Below are model statements investigators may adapt to describe storage and archiving of data. (Please see the devices/apps section for language on data stored on remote device platforms).

---

Sample: Cloud Repository
Investigators will store your data in a controlled-access repository in the cloud. The repository is controlled-access, meaning only certain research team members have authorized accounts to access the data. “In the cloud” refers to servers in a data center that are managed by a third party and accessible through the Internet. Any computing device with access to the Internet could connect to this closed-access repository. We use [X, Y, Z] methods to protect data and methods to ensure data will be used for the approved purpose.

Sample: Cloud Storage
Your study data will be stored in the cloud. “In the cloud” refers to servers in a data center that are managed by a third party and accessible through the Internet. When storing your study data, we will replace your name with a random code on all your study data. The coded data will be encrypted and stored on a secure cloud server under the control of [XX] to prevent improper access.

Sample: Archiving Computer Data
Archiving means saving for use at a later date. Computer data, such as instant messaging files, captured web site records, and copies of electronic mail will be archived. This data will be stored in password-protected files on a computer in [LOCATION]. Archived computer data will be also stored <<insert location>> and locked in a filing cabinet in a secure [LOCATION] with access limited to authorized individuals.