BIOPROCESS ONLINE

Guest Column | December 5, 2018

Startups, Cloud Storage, & Data Integrity: Don't Let This Happen To You!

By Kip Wolf, Tunnell Consulting

Data integrity is of paramount importance to ensure patient health and safety and to improve shareholder value, particularly for virtual companies that depend on the contractual agreements between themselves and their partners and suppliers. Startups finding themselves in the throes of managing complex drug development programs realize they may face great risk if they do not begin with the end in mind and integrate data integrity practices early on. Whether planning a successful filing, a launch, and sustainable operations or working toward an exit strategy of selling the new asset after successful Phase 2 clinical trial results, understanding what robust data integrity means and planning for it early can prevent serious failures down the product development life cycle. Some real-life examples of failures follow.

Failure #1: A virtual company with a new drug in a Phase 3 study was preparing to file the new drug application with the health authority. In preparation for the filing, checks for data integrity and conformance to file were performed that uncovered discrepancies in the reported data (e.g., certificate of analysis, batch records). The sponsor, the multiple contract development and manufacturing organizations (CDMOs), and the many contract testing laboratories were all using various cloud storage and collaboration solutions to store and share data. Without a clear definition, procedures, or agreement on the identification and controls around source/raw data, increased scrutiny and data analysis was required with additional follow-up with the health authority. This delayed the application filing and all related downstream activities by many months.

Failure #2: A project team member from outside the organization, for purposes of project collaboration, was given access to enterprise data in the cloud. Years after the project was over and the team member no longer had any relationship with the organization, he still had access to the project-related enterprise data in the cloud. No one in the organization had audited the user account access or disabled sharing and collaboration for the cloud data after the project was completed.

Failure #3: A startup virtual company, wholly dependent on partner relationships for success (e.g., clinical investigators, contract manufacturers/laboratories), received a negative response from the health authority regarding their new drug application. Clinical trial data submitted to support the application was found to be unreliable and was excluded. The clinical trial sites failed to complete the study under GCP. Investigators at multiple clinical study sites were (at the very least) careless or had intentionally falsified study data before sharing it with the sponsor.

Content Collaboration As A Critical Success Factor

In our modern age, startups cannot afford to manage development programs without cloud storage and collaboration spaces. Most startups rely heavily on partners and outsourcing models, while others operate as completely virtual companies that are particularly vulnerable to inefficiency and ineffectiveness if left without appropriate and secure cloud storage and

collaboration spaces. ("Appropriate" is defined here as both meeting the strategic business objectives and the regulatory compliance requirements.) A contributor to this challenge faced by startups is that frequently the founders, executive leadership, and/or senior management of these very small firms come from large to midsize companies where storage and collaboration spaces are common and managed by someone else (likely a large and capable information technology department). Left to fend for themselves at their new startup, we find that many of these well-intentioned executives and senior leaders default to the cloud storage and collaboration spaces with which they are personally familiar, often using their personal account credentials and free cloud collaboration services (e.g., Google Drive, iCloud).

While finely featured and appropriately accessible for collaborating with family members on pictures for the family photo album, these free services for personal use are not properly provisioned, accessed, or secured to ensure appropriate management of drug development data. These free solutions for personal use typically require endorsement of disclaimers or terms and conditions that rarely include promises related to "up-time" or data loss prevention. However, with the paid variety for business use (e.g., Dropbox Business, Google Drive for Work, Microsoft OneDrive for Business, Box for Business), many of these familiar solutions will negotiate a service level agreement to include "up-time" commitments (in some cases, as much as 99.9 percent), data backup, and restoration services and technical support for business users (to name a few). When negotiating with the service provider, it is also important to ask clarifying questions that may inform the interpretation of the risk profile to aid in making an effective decision that best fits the needs of the startup:

- In what location will the data be stored (e.g., one or multiple sites, on what continents)?
- How will the files be viewed/shared and by whom (e.g., only users with access credentials, or will there be "open" shares for public information and record of who accessed what)?
- What types of files will be allowed (i.e., are there limitations to specific file types)?
- How will the files be protected (e.g., what level of encryption, file splitting, and hashing)?
- How is data storage expanded (i.e., provisioning and paying for more space) or extracted for data migration (e.g., moving to a different provider or transferring to an acquiring company)?

The use of computerized systems is practically unavoidable in today's business world. In addition to data integrity responsibilities, leadership and management in startups must remember that the principles listed in 21 CFR Part 11 apply to clinical study data as much as they do to later commercial manufacturing data. This may include, but is not limited to, source data supporting regulatory filings (e.g., preclinical or clinical study data), institutional review board (IRB) materials (e.g., minutes, procedures), and formal agency correspondence.

Particularly during development phases, collaboration of content and accessibility of data is critically important. Collaboration among the development team and between the team and other key stakeholders such as business management, investors, review boards, and the like is terribly important to the success of the development program. Communication breakdown or delays caused by lack of visibility can have a significantly negative effect on the development program time lines.

"Just Right" Document Control And Records Management

Very often we find that startups apply either too little or too much rigor to document control and records management. For example, waiting until late-stage development to consider formal document control or records management is not recommended (too little rigor). Nor is it recommended to implement a fully robust technology solution (like that of midsize to large drug companies) in early-stage development (too much rigor).

An effective approach for virtual startups is to apply a right-sized solution for document control and records management that will evolve and grow with the drug development life cycle. This includes both controls for internal documents and records and ensuring controls are in place for any partners, investigators, service providers, and the like.

It is recommended that basic procedures for internal document control (e.g., revision history, document recall/supersede, how deletion and unauthorized editing are prevented) be defined early in the drug development life cycle. For example, we find it is more efficient and effective to create internal documents within the basic document control framework than it is to revise legacy documents and retrain staff and support resources later. And it is a GCP of 21 CFR 56.108 that

each IRB "must follow written procedures for conducting initial and continuing review of research and for reporting IRB findings and actions to the investigator and the institution." CROs and IRBs must follow effective standard operating procedures, which include document control requirements that must be verified by the sponsor, as they hold ultimate responsibility for the study.

A basic understanding of records management is also necessary for the virtual startup. While it is true that most of the technical records may reside externally at (for example) investigator sites, contract laboratories, or CDMOs, it is the sponsor's responsibility to ensure records management and retention policies are in effect and operationally executed. It is recommended that basic procedures for records management be established very early, including defining the location of source/raw data for all record types. Document the records management details for both internal (e.g., policies, procedures, interactions with health authorities) and external (e.g., suppliers, CDMO, 3PL) record locations. A matrix of what records are stored where and by whom is of great value for operational integrity, inspection readiness, and data migration in the event of merger or acquisition of either the startup drug company or one of its partners or suppliers.

As stated in 21 CFR 58.195, records for nonclinical laboratory studies must be retained for at least "five years following the date on which the results of the nonclinical laboratory study" are submitted as part of an application to the FDA and for "at least two years following the date on which the study is completed, terminated, or discontinued" for study data results that do not result in submission to support application to the FDA. Other records retention requirements for investigators (21 CFR 312.62) require retention for "two years following the date a marketing application is approved" or "two years after the investigation is discontinued and FDA is notified."

Records sometimes outlast the company that created them, as organizations merge or are acquired. Records must be protected both for good business and as a regulatory requirement. However, accessibility of these records and data is also of importance for partners, suppliers, and prospective investors. Not only must these records be maintained in a way that ensures data integrity, but in most cases, they must also be available upon request by health authorities within a reasonable time to access, copy, and/or verify such records.

About The Author:

Kip Wolf is a principal at Tunnell Consulting, where he leads the data integrity practice. Wolf has more than 25 years of experience as a management consultant, during which he has also temporarily held various leadership positions at some of the world’s top life sciences companies. Wolf temporarily worked inside Wyeth pre-Pfizer merger and inside Merck post-Schering merger. In both cases he led business process management (BPM) groups — in Wyeth’s manufacturing division and in Merck’s R&D division. At Tunnell, he uses his product development program management experience to improve the probability of successful regulatory filing and product launch. He also consults, teaches, speaks, and publishes on topics of data integrity and quality systems. Wolf can be reached at Kip.Wolf@tunnellconsulting.com.