Electronic Data Integrity
IN THE DRUG-DEVELOPMENT PROCESS

IN AN EXCLUSIVE TO PHARMAVOICE, PETER M. SMITH, PH.D., PROJECT MANAGER AT TARATEC DEVELOPMENT CORP., DISCUSSES THE IMPORTANCE OF ELECTRONIC DATA INTEGRITY IN THE DRUG-DEVELOPMENT PROCESS.

A guiding principle in thinking about electronic data integrity is to challenge the system or the data against these points: manual systems cannot be secured; if it is not documented, it was not done; administrative controls and redundant checking are required; and a trained analyst using an approved procedure must generate the data.

IN AUGUST 2003, THE FDA RESTATED ITS GUIDELINES ON 21 CFR PART 11 REGULATION and a more narrow interpretation was given, prompting a more pragmatic approach to electronic data integrity based on risk assessments. **VARIOUS INTERPRETATIONS OF THIS APPROACH REMAIN,** and there are ongoing **DISCUSSIONS BETWEEN THE FDA AND INDUSTRY REPRESENTATIVES AS TO THE LONG-TERM FORM OF THE REGULATION.** Even though the explicit Part 11 rules remain in question, the need to ensure the integrity of electronic data has not gone away.

There are huge costs and time pressures involved in preparing data to support submission to the Food and Drug Administration for approval of a drug candidate before marketing. To avoid any temptation to cut corners or make misguided claims, the FDA reviews and challenges the submitted data for truth and accuracy.

"This is the part of the checks and balances built into any open system," says Peter M. Smith, Ph.D., project manager at Taratec Development Corp. "These checks may appear burdensome and time delaying — submission under regulatory compliance takes at least twice as long as a nonregulated one — but in practice they are necessary to ensure the safety and efficacy of potential drugs and are generally effective in preventing problems."

Using a series of regulations and the tools of the auditor, the FDA challenges submissions to confirm whether the systems do, and can be proven to do, what they are supposed to, and whether the data are secure from falsification and can be proven to be secure.

"The first point here requires system validation, using standards established under the 20-year old GxP standards," he says. "The second point is the thrust of the recent Part 11 regulation."

PART 11 SUMMARIZED

The 21 CFR Part 11 regulation is a relatively short document that was intended to allow the use of computer-managed data in support of new drug submissions to the FDA. Previous regulations required paper documentation. To respond to the rise of electronic data, the FDA crafted Part 11 after discussion with the pharmaceutical industry, and it became law in 1997.

"It may have been a short regulation, but it had major consequences, and a large industry developed to provide guidance, assessments, and implementation services to ensure that systems and instruments complied with the requirements of the regulation," Dr. Smith says. "The costs of such compliance to the pharmaceutical industry soared into the billions of dollars, and in August 2003 the agency restated its guidelines on Part 11 and a more narrow interpretation of Part 11 was given."

In response, a more pragmatic approach based on risk assessments was proposed; the regulation is most enforced in those areas of the greatest risk to safety and health, according to Dr. Smith.

"Many regulatory departments in pharma took this to mean the demise of Part 11 and indeed, there are ongoing discussions between the FDA and industry representatives as to the long-term form of the regulation," he says.

He adds, however, that the basic principles behind Part 11 remain sound, have been recognized for many years, and indeed are implicit in many previous regulations.

"Part 11 was never a stand-alone requirement but rather was meant to be an extension of the existing predicate rules to include electronic data; it was an enhancement to the validation requirements for systems," he says. "So even if the explicit Part 11 rules are in question at this time, the need to ensure the data integrity of electronic data has not gone away, whether under Part 11 guidelines or earlier rules for data integrity under GCP, GLP, and GMP standards.

"Simply put, Part 11 is designed to ensure that modern electronic records have the same validity as paper records," Dr. Smith says. "Alterations to paper records are readily observed and the physical records themselves can be challenged if necessary by a range of forensic tests. Explicit changes are signed and dated. But today there are more electronic data than paper data, and changes in computer data are not susceptible to forensic tests."

To ensure data integrity, the Part 11 regulation asks for audit trails and electronic sig-

natures. The audit trail tracks any change to the data and records who, what, when, and why. The electronic signature ensures that the people who are making changes are who they say they are. Dr. Smith notes that recording the reason for making a change is not actually required by the Part 11 regulation but it is a good laboratory practice (GLP) requirement, per 21 CFR 58.130(e) and as such is usually included in Part 11 compliance assessments.

"With these controls in place, the agency will accept electronic data as readily as paper data, with great efficiencies realized by all," Dr. Smith says.

IN PRACTICE

To provide an audit trail in electronic database systems that complies with Part 11, a best practice is to develop a general utility that is globally available, flexible to various system designs, and applicable to existing databases as needed. Further, this tool should be certified by a company's Part 11 project-management office responsible for ensuring regulatory compliance.

The general approach is to create an audit table in the database, which is a shadow of the main (source) database table. In that audit table the original record and a record with any changes made to the source are stored. Triggers are used to initiate a new record.

"There are two ways to do this," Dr. Smith explains. "The first is the column-based model, which records each change to a database field. For example, if three fields changed in a record then there are three records in the audit table. The second method is a row-based model, whereby each record is recorded when it is changed and only one record gets added to the audit table, even if three fields get changed in the source record. Since both models save the initial record as well, the number of audit records created is effectively doubled."

The column-based model allows easy tracking of value changes, and the original records can be programmatically reconstructed.

The row-based model gives a much easier history of the record but it is not so easy to track separate value changes. It is more suited to voluminous research data. Depending on the initial database design and the requirements of the audit, either model is acceptable, or both can be used at the same time.

REMOTE USERS

Dr. Smith says companies that work in a straight database environment can easily track who makes changes and when through the database security mechanism that defines access roles and identities of users. Although, in this type of system local times have to be converted to GMT to provide an unambiguous standard time stamp. The shadow audit table records the old and the new data, he explains. Reasons can be requested and written to a field in the audit table.

"But modern computing environments are not usually homogeneous, and if companies want to take advantage of a three-tier computing hierarchy — user-interface, middle-tier of logic and access, and the database repository — then there is a need to manage the user identity across these heterogeneous layers," he says. "This can be done, but it is not easy, especially if there is a requirement, at the same time, to exploit the database roles already built into the system, and on which database administrators rely. The final result is a complex but transparent mechanism that populates the shadow audit table."

WRAPPER SOLUTIONS

"One final issue should be discussed, and that is the problem of dealing with popular desktop tools that manage data and how to ensure the integrity of data in this environment," Dr. Smith says. "In particular, Microsoft Excel has wide currency but there are no obvious ways to secure these data from change."

The industry has responded to this problem with systems that do, in fact, secure such data by "wrapping" Excel in software that records changes and does not allow unauthorized data manipulation. This software typically implements a secure central service that tracks the files and data changes and which users — in a regulated environment — have logged in to access Excel.

"To the users, Excel behaves normally, but any changes are recorded when the spreadsheet is saved, and an audit trail for that file is developed," he says. "Such systems often are extended to incorporate data capture from scientific instruments by taking the data stream, filtering it, and securing it before it is analyzed by Excel or another tool. When properly configured, such wrapper solutions provide full Part 11 compliance from instrument to database."

"There are several vendors of such software; it's not so much what they do that is important when evaluating them, but how they do it, for example, how nonobtrusive the software appears to the user," Dr. Smith adds.✦

To provide an audit trail in electronic database systems to comply with Part 11, a best practice is to develop a general utility that is globally available, flexible to various system designs, and applicable to existing databases as needed. Further, this tool should be certified by a company's Part 11 project-management office responsible for ensuring regulatory compliance.

PharmaVoice welcomes comments about this article. E-mail us at feedback@pharmavoice.com.