

Computer Systems Validation, Part 2: Installing GCP Systems at Investigator Sites

Teri Stokes

Regulatory authorities expect investigator sites to be in control of all computerized systems, devices, and instruments to ensure the integrity of data such systems generate. Here are guidelines for ensuring that such systems are operated to GCP standards for validation and change control.

The use of computers has become so much a part of everyone's daily work experience that it is often taken for granted. Computer equipment and software are thought of in much the same utilitarian and passive way as phones, faxes, calculators, and typewriters. Although computers can perform all the data handling functions of the devices mentioned above, there is one major difference with computerized systems, and that is their capacity for complex data management without the participation of a human being.

Computerized systems can gather, store, retrieve, transform, and communicate huge amounts of data independent of human intervention, to the point that human operators can lose a sense of what the data mean or how they should look. From body

scans and digitized X rays to digital readouts from treadmills, medical decisions are being based on data generated by computerized systems where the focus is on the medicine of the system and not the computerized element. It becomes easy to assume that the data on a printout are correct just because they are on a printout. In reality, this may not be the case if computerized systems are operated without good clinical practice (GCP) standards for validation and control of changes.

Regulatory authorities expect the management at an investigator site to be in control of all computerized systems, devices, and instruments associated with the delivery of patient care. They are concerned about the integrity of data on such computerized systems, because health care is most safely and effectively delivered in the context of information about the patient's medical history, treatment record, and reliable diagnostic data.

The accessibility and integrity of data is best supported by installing and maintaining reliable systems that perform as expected every time they are used. When regulatory authorities and sponsors come to inspect or audit, they want to see documented evidence of the quality of such computerized systems. The four major considerations when installing GCP systems at investigator sites are

- data integrity
- system reliability
- management control
- auditable quality.

Data integrity

Data integrity is the *raison d'être* of GCP for computerized systems installed at investigator sites. In fact, it is the character of the data stored on the system disk or handled by the application that defines a GCP system (see Definition of Terms box). If the data are used as source data for a case report form (CRF) or are otherwise used to prove the safety, efficacy, or quality of the study therapy, then they are classified as GCP data. The software handling such data and the platform system that allows the software application to work are then considered to be GCP systems and are subject to validation.

Teri Stokes, PhD, is senior consultant and director of GXP International, 131 Sudbury Road, Concord, MA 01742, (978) 287-4393, fax (978) 369-8907, gxpintl@ma.ultranet.com.

To protect and ensure the integrity of GCP data in computerized systems, it is necessary to consider several concepts. Virus protection is very important for personal computer (PC) systems at investigator sites. The daily and ongoing use of virus checkers is one key to peace of mind. A designated “GCP PC” can be further protected from virus infestation by adopting a standard operating procedure (SOP) for system security that forbids the use of personal diskettes for private programs, such as games, or for Internet access or downloading materials. It can also have password and code protection to ensure that only authorized users have after-hours access.

When any GCP application or platform system is installed, a number of issues should be addressed and their resolution documented to protect the integrity of GCP data on the system (see Protecting Data Integrity box).

System reliability

The reliability of a computerized system rests upon three factors: the quality built into the system during its development and testing by the manufacturer, the installation of the system to specified conditions at the investigator site, and the configuration management during the system’s operational use, with special attention given to maintenance activities and change control.

Three concepts from the world of good manufacturing practice (GMP) can also serve GCP interests very well during system installation:

Installation qualification (IQ). Documented verification that all key aspects of the installation adhere to approved design intentions, according to system specifications, and that the manufacturers’ recommendations are suitably considered.

Operational qualification (OQ). Documented verification that each unit or subsystem operates as intended throughout its anticipated operating range.

Performance qualification (PQ). Documented verification that the integrated system performs as intended in its normal operating environment.¹

In lay terms, IQ means that you

Protecting Data Integrity

To protect the integrity of GCP data, the following questions should be addressed when installing a computerized system or a new application.

- Who is authorized to enter data in the system? edit, calculate, or transform data? retrieve and change data? approve data? Where are the written instructions or standard operating procedures (SOPs) for performing such tasks on the system?
- Does the system have an audit trail function? Is it to be activated? If not, why not? (Some audit trails can slow performance to unusable levels.)
- If no audit trail function exists or is to be used, how is unauthorized access to or use of GCP data in the system to be prevented and monitored?
- Does the system have internal range and logic checks for data? How can such checks be tested to ensure that they work properly?
- Does the new system transmit data to another system or to another site? How can the completeness and accuracy of its data transmissions be checked?
- Does the new system transform data through calculations? Can these calculations be checked by another method?
- Does the system fill in “missing” data, such as sequential label numbers or visit dates? Can this function be turned off at installation if it has a negative impact on the accuracy of GCP information?
- What is the backup procedure and strategy for GCP data handled by the system? Where are backup copies of the data to be stored? How are they to be protected from fire, flood, and other perils? What constitutes sufficient backup of the platform system software, so that data can be read and properly retrieved from backup copies on tape or disk?
- What is the procedure for collecting, processing, and using GCP data during times that the new system is unavailable to the site? What is the procedure for resuming work with the system when it is again available? How are the interim data to be handled by the system—manually entered, scanned in, referenced as paper?

followed the installation instructions that came with your new system. That includes making sure that your physical location meets the installation conditions specified in the system documentation for such factors as air conditioning, low moisture, power, and room conditions. It also means that you made sure all supporting software (databases, operating system, and tools, for example) were the correct versions specified for your new system. IQ answers these questions: Does the system power up properly? Do the right screens come on?

OQ tests the built-in capabilities of the new system. In OQ you focus on specific functions, know the operating range for each function, and then develop ways to test those limits—testing both normal and problem data that are right at, just above, and just below the range limits. If you expect

the new system to handle pH values, for example, then you would try to enter pH values of −1, 0, 1, 13, 14, and 15, and then record the way the system reacted to those values. OQ answers the question, Do key functions of the new system operate correctly in and of themselves?

PQ is an approach to testing the new system as a whole in its everyday environment, with users doing various tasks on it. PQ also tests the new system’s interaction with other systems for transmitting, receiving, and retrieving data. PQ also looks at overall issues. For example, do important functions of the system operate as they are described in the system manual or in your own SOPs? Again, PQ tests the new system with normal and problem data and stress situations that will show how it responds in your active clinical climate.

What happens if a new person tries to log on to the system without a password? Is the person allowed in or kept out by the system? What happens when an operator presses a letter instead of a number in a critical numeric data field? Does the system recognize the error or ignore it? How does it handle the data item? Does the error message make sense in the context of the situation, and does it look the same as described in the system's user manual? PQ is a way to test the new system for its ability to perform in your real work situation.

System logs. In addition to IQ, OQ, and PQ testing, system logs are important to a new system's reliability and should be established at the time of installation. The system logs can be in several sections of the same notebook or in separate record files—whichever is more convenient. The logs provide a place to record activities as they are performed on the system and should be located near the system itself for ease of use. Logs provide documented evidence of system quality control (QC) activities. Six essential logs cover configuration, maintenance, change control, backup and recovery, problems, and testing.

Configuration logs identify and record every software and hardware component of the GCP system, such as the operating system, GCP applications, databases, tools, disks, modems, and network routers. A configuration log should include maps that identify the software on each server or PC system and network

Investigators and CRCs have the same responsibility for electronic data as they do for data collected on paper.

connections between systems and between sites for GCP applications. It should include flow charts showing how various GCP applications interact, and it should be updated to reflect changes.

Maintenance logs document installation, service calls, repairs, and component replacements. They should include supplier maintenance contracts for system components.

Change control logs are a record of all changes to hardware or software components, such as software upgrades, bug fixes, and new versions of the system. They should include

approval signatures and dates for medium to large changes to the system.

Backup and recovery logs are for recording system and data backup activities and any use of backup tapes for system recovery purposes. They should include a schema for making backups—daily, weekly, monthly—and the storage location of backup tapes and disks.

Problem logs are used to record user concerns and technical problems, track errors, and document their resolution. They should describe the normal resolution process, for example, whether to use supplier support services or internal processes as specified in the SOP.

Testing logs are used to record formal testing activities and retesting after medium to major system changes. They should identify the item or items tested, the extent of the testing performed, the date it occurred, and signatures of the tester and a witness.

Every system log, regardless of topic, should include the following key section items:

- a description of the log's issue and any requested action
- a description of decisions taken and actions performed
- the signature of the person performing the action and the date the action took place
- the system manager's signature and date to confirm the decision and/or action if taken by another.

Definitions of Terms

computerized system. The combination of a software application with its supporting electronic platform and the interactions of the application with its users and/or associated equipment to perform work in the clinical environment.

GCP data. Any data used to prove the safety, efficacy, or quality (SEQ) of a medicinal product or clinical therapy that is the subject of a clinical study.

GCP system. (1) Any software application or computerized

hardware, device, or instrument that collects, stores, calculates/transforms, retrieves, reports, transmits, or archives GCP data. (2) Any computerized system that controls the delivery of therapy in GCP studies—for example, medical implants or radiation dosage systems.

GCP application system. Any application software used to handle GCP data—for example, patient history systems, laboratory analytical systems, pharmacy supply tracking systems, dosage calculating systems, or diagnostic device systems.

GCP platform system. A platform system that supports at least one designated GCP application.

platform system. All the computer components required to enable a software application to perform its intended function—for example, the operating system, the central processing unit (CPU), hard disks, floppy-disk drives, printers, modems, databases, tools/drivers, network routers, and communications software.

Management control

To exert control over a computerized system, investigator site managers

- ensure that computerized systems are suitable for their intended purposes
- ensure that the facilities, equipment, and data handling procedures are of adequate quality
- appoint, train, and effectively organize an adequate number of competent staff members to use computerized systems to GCP standards.
- designate qualified personnel with specific responsibility for development, validation, operation, and maintenance of computerized systems to GCP standards.

For specific clinical studies, the investigators and clinical research coordinators (CRCs) should be fully aware of any computerized systems used in the conduct of studies under their direction. Their responsibility for data recorded electronically is the same as that for data recorded on paper. Therefore, only validated systems should be used for GCP studies.

When an investigator site intends to install a new GCP software application or hardware system, it should write a system quality assurance plan that addresses the four responsibilities listed above. This does not have to be a huge document, but it should address site managers' GCP responsibilities by documenting answers to questions in the following categories.

Ensure that computerized systems are suitable for their intended purposes. For what purposes will the site use the newly installed software application and/or computerized hardware, device, or instrument? Which of those purposes are GCP-oriented? With what other manual or automated systems must this new system integrate at the site?

What functions of the new system support the site's intended GCP and non-GCP purposes? Are there any special needs for replacing an existing system with this new system or for writing interface software to allow the new system to communicate with other systems at the site? How will such special needs be fulfilled?

Ensure that the facilities, equipment, and

Validation's motto
is simple: If it isn't
documented, it didn't
happen.

data handling procedures are of adequate quality. Where will the computerized system be located?

For computerized hardware, devices, and instruments. Is enough physical space available? Is there adequate control of temperature, humidity, and power supply to meet the manufacturer's specifications? Are new modem or electrical lines needed? Is there proper grounding to protect users and patients? Should spare parts be kept on hand for backup purposes? What physical security measures will be taken to protect the system from theft, vandalism, and unauthorized access?

For software applications. Does the site's system meet the software manufacturer's requirements for logical space? For example, is adequate memory and disk storage space available? Is this version of the new application compatible with the existing versions of the platform system's components—such as the operating system and database—or are upgrades needed for some items? Are special printer or modem drivers needed? Where will the master copy of the software application be safely kept? What about a working backup copy to use for recovery in case of virus contamination?

Do the manufacturer's system manuals and user instruction materials provide enough guidance for training users at your site, or are they too technical and confusing? Is the application's on-line help function

sufficient to guide users in operating the system, or do they also need an instruction sheet in the work area? What new SOPs need to be written for system support activities or the use of the new system? Does the supplier offer training courses?

Appoint, train, and effectively organize an adequate number of competent staff members to use computerized systems to GCP standards. Who will be the primary users of the new system? How will they be trained in system use? What materials (such as SOPs, instruction sheets, on-line help, technical support hotlines) will be used to support training on and production use of the new system? How will users' compliance with the proper procedures for the GCP system be checked?

Who will resolve work issues that arise from the use of the new system? To whom will users report problems with the system? How will system access and data edit authorization rights be administered? Will any special transition procedures be used during the conversion to the new system—for example, will continuing records be kept on the prior system and all new records be started on the new system? What manual backup and recovery procedures will users rely on during times when the new system is unavailable? How will users be trained in GCP principles for using computerized systems?

Designate qualified personnel with specific responsibility for development, validation, operation, and maintenance of computerized systems to GCP standards. Who is the system-responsible user for the new system—that is, the person who trains the other users, designs work-related functional tests for the system, and validates the system for production use? Who is the technical support person who installs, supports, and maintains the new system and executes technical tests to validate the system's technical operation? Who developed the new system? Who fixes bugs, updates software, and handles hardware problems for the new system? What role, if any, will the system suppliers play in ongoing support and maintenance? How will physical and logical security be implemented to protect the hardware,

software, and GCP data?

Auditable quality

The basic concept underlying audits and inspections is that documented evidence must be seen in order for actions to be believed. “If it isn’t documented, it didn’t happen”—that’s the motto. When management is in control, written policies, plans, logs, and SOPs will be in place to describe how the system is being used and how the organization is protecting GCP data.

If users are to be trained and to know how to use the system, user materials, training records, and SOPs should be available. When a system is properly installed and managed, system logs will document decisions and actions taken on the system and its data handling activities. The key to auditable quality is documented evidence.

Providing documented evidence of a system’s quality during its development is the responsibility of the system supplier, but providing documented evidence of the quality of GCP systems in clinical use for studies at an investigator site rests with the site. This responsibility usually includes systems purchased by the site that are used for handling GCP data or for computerized control of activities involved in the delivery of therapy. This means that the site is responsible for identifying its GCP systems and for validating them according to written plans and procedures.

When sponsors provide systems to

Definitions of Terms

computerized system. The combination of a software application with its supporting electronic platform and the interactions of the application with its users and/or associated equipment to perform work in the clinical environment.

GCP data. Any data used to prove the safety, efficacy, or quality (SEQ) of a medicinal product or clinical therapy that is the subject of a clinical study.

GCP system. (1) Any software application or computerized hardware, device, or instrument that collects, stores, calculates/transforms, retrieves, reports, transmits, or archives GCP data. (2) Any computerized system that controls the delivery of therapy in GCP studies—for example, medical implants or radiation dosage systems.

GCP application system. Any application software used to handle GCP data—for example, patient history systems, laboratory analytical systems, pharmacy supply tracking systems, dosage calculating systems, or diagnostic device systems.

GCP platform system. A platform system that supports at least one designated GCP application.

platform system. All the computer components required to enable a software application to perform its intended function—for example, the operating system, the central processing unit (CPU), hard disks, floppy-disk drives, printers, modems, databases, tools/drivers, network routers, and communications software.

investigator sites—such as remote data entry (RDE) and electronic patient diary (EPD) systems—the primary responsibility for validation rests with the sponsor that provides those systems. Even so, investigator sites must work with sponsors to plan how such sponsor-supplied systems will be maintained to GCP standards during their use at the sites.

Investigator sites should request the sponsors’ assistance with templates for SOPs and other documentation required for site GCP compliance. Sponsors that bring computer technology into clinical studies

without providing GCP validation support should be closely questioned by investigator sites about validation concerns and GCP compliance.

Part 1 of this series (“Software Purchase and GCP Compliance”) appeared in the September 1996 issue. Part 3 will discuss the content of GCP system validation packages.

References

1. T. Stokes, R.C. Branning, K.G. Chapman, et al., *Good Computer Validation Practices: Common Sense Implementation* (Interpharm Press, Inc., Buffalo Grove, IL, 1994), pp. 281–282. □

