The information age has arrived. It is therefore essential to define appropriate conduct and to characterize how we manage expectations in this new operational landscape of our environment. The increasing need to effectively use electronic data systems for efficiency and control is inevitable, and competitive advantage will be directly related to and dependent upon appropriate responses to the new stimuli. Only those who adapt effectively will evolve and prosper. As we journey into the future, we must exercise care that we think our way into a new way of acting rather than acting our way into a new way of thinking.

The watershed 1997 “Electronic Records; Electronic Signatures” rule (ERES), 21 CFR Part 11, is now both gatekeeper and enabler of an increasingly electronic landscape (1). The rule stipulates stringent controls concerning the use of electronic records and signatures, and more importantly, it defines the requirements acceptable to FDA for capture, storage, retrieval, maintenance, and data security. This article focuses on the importance of auditing and validating electronic systems as a consequence of the rule. It frames the regulatory risk, integrates the ERES component, identifies new skills that will be required in the information age, and provides an audit process model to help mitigate the liability exposure of management.

The Regulatory Environment

FDA is the nation’s oldest consumer protection agency, overseeing more than 100,000 companies producing products valued in excess of one trillion dollars. Regulations mandating accountability and traceability throughout drug development, manufacturing and distribution are the foundation of FDA’s enforcement power. In the pharmaceutical sector, regulatory risks affect the organization directly and include FDA 483s, warning letters, and consent decrees. These actions can result in nonapprovals of pending new drug submissions, delayed approvals of new products, and/or loss of government contracts. Legal risks include injunction from manufacture, search of premises, seizure of products and records, and prosecution — corporate or individual, civil or criminal. Regulatory and legal penalties include fines (individual and corporate), sanctions, and imprisonment. A business can lose market share and/or its good name while bearing the cost of litigation or remediation. Particularly severe penalties could ultimately put an organization out of business. Individuals can lose even more.

The body of regulations is dynamic and changes as products and technologies evolve. Different regulations address different stages of the product life cycle, from good laboratory practices (GLP) through discovery and preclinical development, good clinical practices (GCP) through clinical trials, and finally good manufacturing practices (GMP) through clinical drug substance and drug product manufacture and postapproval manufacturing and distribution. It might appear to be easy to nestle isolated regulations into the functional silos defined by the development process, but real integrated risk assessment begs cross-functional interpretation; that is, GxP, where GLP + GCP + GMP = GxP. There are many “interpreters” of the regulations in industry and in government, but no quantifiable models exist, and interpretation is usually an amalgamation of knowledge, experience, and often serendipitous timing.

FDA enforcement is predicated on human efforts and consequently follows discernible patterns. Even though regulations and guidance documents provide the framework for quality systems, many areas still require judgment. Inspectors identify and target specific areas of primary interest (such as validation, adverse event reporting, and equipment cleaning). They then focus on unearthing examples of those concerns and obtaining evidence. Adverse findings can negatively affect industry reputation, profits, and shareholder confidence.
**The Rule**

The ERES rule (printed in *BioPharm’s November 2000 supplement, pp. 62–64*) is divided into three sections: Subpart A, General Provisions; Subpart B, Electronic Records; and Subpart C, Electronic Signatures. It is important from the outset that you clearly understand the distinction between records and signatures. Records are “any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.” Nonconformance with the electronic record rule means you are in nonconformance with the original record-keeping requirement of the predicate regulations.

**Signatures.** Under the regulation, signatures can appear in three manifestations — handwritten, digital, and electronic — defined in 21 CFR 11.3 as follows. A handwritten *signature* is “the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form.” That scripted name or legal mark can be applied to devices other than paper. A digital *signature* is “an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.” An electronic *signature* is “a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s signature.”

Electronic records and signatures can be used in accordance with Part 11 unless paper records are specifically required by a particular regulation. In surprisingly sweeping language, the agency applies those criteria to all records in electronic form under any requirement within any FDA regulation. As with computerized process controls elsewhere, the “record/signature” computer system (hardware and software), controls, and relevant documentation must be available for review during FDA inspections. The rule identifies two environments: In closed systems, access is controlled by people who are responsible for the content of electronic records on the system. In open systems, access is not controlled by people who are responsible for the content of electronic records that are on the system. The applicable controls for each environment differ in direct relation to the presumed layer of security.

**Closed systems** require specific procedures and controls to ensure authenticity, integrity, and confidentiality while preventing the signatory from repudiating the signature. The rule requires human readability and retrievability. The agency has clearly stated it intent to inspect, review, and copy records. Procedures should ensure that personnel are qualified, that records are maintained accurately and completely, that access to the system is limited to authorized persons, and that records are protected throughout the retention period. The record must have audit trails that are secure, operator independent, computer-generated, and time-and-date stamped. Audit trails should include the creation, modification, and deletion of records without overwriting or obscuring previous information. Periodic performance of operating system checks, authority checks, and device checks to ensure system, record, and data integrity are mandatory. Controls on system documentation should include distribution, access, use, revision, and change control. They must be validated to ensure accuracy, reliability, and consistency. Ultimately, your procedures and controls must hold personnel accountable for their actions and deter record falsification.

**Open systems** need all the controls required for closed systems but contain additional measures (such as document encryption and digital signal standards) to ensure authenticity, integrity, and confidentiality. Electronic records that are signed must adhere to the controls listed for them and must also include the printed name of the signer, the date and time of the signature, and the purpose of the signature (such as review or approval). The signatures and records must be human readable by display or printout.

Electronic signatures and handwritten signatures must also be linked to ensure that signatures cannot be excised, copied, transferred, or falsified. The identity of individuals must be verified, and signatures must be unique to an individual and not reassignable. Additionally, organizations that intend to use electronic signature systems must certify to FDA their intent to do so before or at the time they begin using the system. “Affidavits of Certification” must be submitted in paper form and attest that signatures are legally binding. A field notice directs investigators to check the Office of Regulatory Affairs (ORA) intranet site to determine whether an electronic signature certification has been filed before arriving at an inspection site (2).

**Nonbiometric signatures** must contain at least two different identification components (such as user ID and password). *Biometric signatures* verify an individual’s identity based on measurement of the individual’s physical feature(s) or repeatable action(s) in which those features and/or actions are both unique to that individual and measurable. Applications for which a single sign-on accesses multiple tasks should use all identification components at first, with partial identification for each task thereafter. Applications for which multiple sign-ons are used without unrestricted access require all identification components to be used each time. Only the owner should use nonbiometric signatures, and the organization should ensure that use by other individuals is precluded and does not occur without the collaboration of at least two or
more individuals. Biometric signatures need only ensure use by the owner. Identification codes and passwords must be procedurally administered.

Systems using electronic signatures must have controls to ensure their security and integrity. Controls should include assuring that no two individuals have the same combination of identification code and password; periodic checks, recalls, or revisions of identification code and password; loss management and replacement procedures; testing of devices (tokens or cards) that produce or maintain identification codes or passwords to ensure proper function and unaltered state; safeguards against unauthorized use; and urgent and immediate reporting of unauthorized use attempts to the security unit and/or management.

Compliance with the ERES rule focuses on three fundamental elements: a computer generated audit trail with local date/time stamps of user entries and actions that create, modify, or delete a record; security practices that limit access to authorized users, hold users accountable to written policies, and that differentiate between open and closed systems; and modalities to ensure retention, retrievability, and reproducibility so that electronic records are archived in electronic form on durable media with accurate transcriptions or complete copies of the data and metadata.

The Operational Landscape
In the medical device industry, the requirement to conduct internal quality assurance audits is specifically promulgated in U.S. regulations (3).

Management responsibility. Quality system regulations (QSRs), 21 CFR 820, charge management with executive responsibility for establishing a commitment to quality, and manufacturers are specifically directed to provide adequate resources to meet the expectations of the regulation. Management has the responsibility to establish procedures for audits, review the results, and when audit findings reveal noncompliance with the requirements, management must take corrective action (see the “Symptoms of Regulatory Danger” box). The QSRs also require verification or validation that corrective and preventive actions are effective, and FDA inspectors are trained to solicit information regarding senior management’s involvement as a routine part of their investigations. Clearly, FDA expects executive management to be involved with and responsible for all aspects of the quality system. Off the record, some FDA officials have hinted that the QSR template may be the model for future revisions to the GMPs and GLPs. That focus highlights FDA’s expectations for executive management.

The enactment of ERES and the increasing regulatory preference for QA systems adds further complexity to the management of computer and documentation systems. FDA believes that the risks of falsification, misinterpretation, and unauthorized change (without leaving evidence) are higher with electronic records than with paper records, and that, therefore, specific controls are required. Requirements are strict for organizations choosing to use electronic modalities, but establish only the minimum requirements for logical, procedural, and physical controls surrounding the use of computers. Clearly, the regulators have certain expectations, and the onus is on industry to create and establish appropriate controls for maintaining record and signature integrity that will satisfy those expectations.

FD&C compliance. Personal responsibility is a hallmark of the Food, Drug, and Cosmetic (FD&C) act, which reflects a core value of FDA compliance and enforcement policy. Legal proceedings almost invariably identify individuals as the defendants under the theory that they actively participate in the unlawful conduct, allow it to happen by passively tolerating violations, or fail to take steps to learn that violations are occurring. Company executives often react with surprise and sometimes anger at being personally associated with the wrongdoing that brought their organization to court, believing that it was a corporate problem only that should not affect them directly. FDA has defended that policy three times in the Supreme Court and has prevailed each time. Executives have been sentenced to prison, disbarred, and fined for their misdeeds.

The Audit
Most pharmaceutical and medical device companies perform quality audits of their internal operations, contractors, and suppliers at some level. Also, many professional and industry organizations and consultants routinely provide assessments and independent third-party audits. Practices are well-recognized within the industry, and inspections typically follow a systematic approach. The “Systems to Be Audited” box on page 36 lists those operations that are usually identified in a quality audit.
Quality audits are often very focused in their performance and in the distribution of the findings. Quality assurance, operations, and procurement departments review the results. Realistically, that information never leaves the protection of operations and rarely reaches the executive level — the very people who are on the liability firing line.

Printout and electronic record differences. As we find more processes that can be linked to electronically generated records and documentation, auditors will encounter new challenges. Electronic data are intangible, a series of magnetic or optical—magnetic impressions on durable media that require machine transposition to become readable by humans. And auditors are human, not cyborgs. Fingers, although tactile and soft-wired to a central neural ganglion, cannot plug into a machine and upload data to the brain. The logical alternative is to print hard copies and verify data points between the database and the source document. But that is not truly auditing the electronic record. A printout of an electronic record is not the actual electronic record. An electronic record has search and sort capabilities, can have algorithms, and contains metadata about the users’ changes and the time and date those changes were made. These metadata are not present in the printout.

That difference is particularly problematic in audits of development processes in which many participants generate quantities of data. The complexities associated with product development and design control with the increasing reliance on computer-generated drawings, spreadsheets, reports, and test data exacerbate the difficulties facing auditors when they wade through an organization’s knowledge architecture, attempting to verify data integrity.

An Audit Solution
So how can you audit electronic data? It cannot be seen; it cannot be touched; and special devices are needed to interpret it. Very simply, you do not: You do not audit electronic data. You must audit the process and ensure that all the supporting systems are properly validated so that they generate verifiable, trustworthy data.

FDA’s acceptance of data from electronic records for decision-making depends on the agency’s ability to verify the quality and integrity of that data during on-site inspections and audits. To be acceptable, the data should meet certain fundamental elements of quality whether collected and recorded electronically or on paper. Data should be attributable, original, accurate, contemporaneous, and legible. Electronic data are generated using computers and computer systems. FDA has long required that all computer systems be properly validated, and the agency intends to apply the same validation concepts and standards to electronic records and signature systems as it does to computer systems.

FDA defines computer validation as providing documented evidence and assurance that computer systems that “touch” the process perform in a reliable and repeatable manner. That requires written
proof that the computer system is suitable for use, is reliable and will continue to be so, functions as it purports to do in the system’s documentation, is secured and protected from unauthorized access, is maintained in a controlled manner, and is protected against uncontrolled change. In manufacturing, “Failure to comply . . . shall render the drug adulterated . . . and such drug, as well as the person who is responsible for the failure to comply, will be subject to regulatory action” (4). The audit process, therefore, is a systems audit like any other system audit. The exception is that this audit requires specialized information technology (IT) and technical skills to evaluate the quality and the fiduciary and security requirements of the information system. Those skills are in addition to the audit skills mentioned and required for other system audits. The “ERES Checklist” box on page 39 lists typical questions and tasks involved in the data system audit.

**Dynamic Knowledge Architecture**

Organizations must establish a knowledge architecture that acknowledges changing needs, meets compliance requirements, and engenders a new paradigm using and managing the complex information highway. The task before management is to effectively bridge the gap between the objectives and values expressed by upper management and the processes and behavior exercised at lower levels into a coherent compliance risk management strategy. A successful effort must ensure protection of the organization and its people from regulatory sanctions. You cannot inspect quality into a product, and you cannot audit integrity into data. You need to build in quality and integrity at the design stage — and that design process can be audited and evaluated to ensure that risk exposure is appropriate and cost-effective.

Organizations and people do not like surprises. Just as there are financial audits to reduce business risks, there need to be audits to reduce electronic and computer risks. FDA has the authority and the power to maintain the public welfare through its inspection program. Recently, the agency exercised its power and authority by assessing multimillion dollar fines and withholding new product approvals until manufacturing and validation problems with products already on the market were resolved. Regulatory issues, therefore, have been escalated to business financial issues.

Although the 21 CFR Part 11 regulation does not appear on the surface to be that challenging, and many organizations have adopted a “wait and see” philosophy, it is a major event worthy of action to avoid unnecessary risk exposure. This is because any violation of 21 CFR Part 11 equates to a violation of FDA predicate GMP, GLP, or GCP regulations. Therefore organizations must think about new ways of acting, or unanticipated exposure could materialize.

**References**


