

2005, Volume 08, Issue 1

Will Your Company's Electronic Records Storage Withstand Legal Scrutiny?

New U.S. and global compliance regulations require stricter maintenance of accurate and trustworthy record keeping.

Charla Griffy-Brown, PhD, Stepheni Bodo, and Linnea McCord, JD

Questions such as those above are important now that global government regulations are increasingly making firms responsible for the accuracy and trustworthiness of their information.

If someone hacks into your company's computer system, would you be able to prove to your customers and shareholders that the integrity of your data—and theirs—had not been compromised? If accusations were leveled at your firm regarding alleged shady accounting practices, could you defend your information processes and their reliability?

The risks of improper retention and management of records have grown substantially with newly passed laws, such as the Sarbanes-Oxley Act of 2002, the Gramm-Leach Bliley Act ("GLBA"), and the European Union Data Protection Directive that incorporate increased fines and jail terms for both private and public entities and their management. This legal and regulatory evolution, when coupled with the explosive use of digital systems to manage modern corporate activities, means that electronic records are now being defined in laws and regulations as being equal to traditional paper and micrographic records.

Therefore, it is important for both private and public entities to reduce the legal, regulatory and business risks involved in the capture, storage, management, and reproduction of their electronic records. Industries at high risk for litigation or regulatory review must be extra vigilant. Concerns include reliability and accuracy of retained records, methods of retention, and ability to retrieve records when required.

Legal and Regulatory Requirements

In order to comply with laws such as these, a firm must retain information in a manner that lets it be quickly retrieved, while still being able to demonstrate that the data have not been altered or even accessed by anyone other than authorized persons. Such requirements mean that the chief information officer (CIO) and legal counsel must work together to ensure competitiveness and compliance at the most reasonable cost.

The legal and regulatory acceptance of electronic records is predicated on these records meeting certain well-established requirements. The overriding requirement is that records are authentic and can be deemed to be reliable, trustworthy and accurate. The implication of this requirement is that the electronic record must have been captured at or near the time of the event or transaction^[1] and must be complete and available for retrieval as requested for regulatory or business purposes. The context and the structure of the electronic record must also be preserved for the full retention life of the record, including any migration of the record from one system or medium to another. Failure to implement these requirements can lead to questions about specific records and the process by which they were managed.

The fewer weaknesses found in the storage and management of the record over its life cycle, the greater the likelihood that the record will withstand any legal challenges regarding its admissibility and, most importantly, its credibility.

Electronic Storage Reliability

The Uniform Photographic Copies of Business and Public Records as Evidence Act (there are both federal and state versions) states that a reproduction made by any "process which accurately reproduces or forms a durable medium for reproducing the original . . . is as admissible in evidence as the original itself."^[2] While most new data stored in the past decade are electronic, many organizations are still converting information from hard copies, so mixed data storage modes are being utilized. For example, many companies store scanned documents and electronic/hard copy faxes in addition to completely electronic exchange storage, such as email.

This act is important because it bridges electronic and hard storage. It also helps to define what is considered "an original" document. Therefore, with the advent of electronic records, the interpretation of a "durable medium" has expanded to encompass electronic storage media. For a reproduction of an electronic record to be as acceptable as the original, the medium used for the storage of records must be reliable and must support the reproduction of an accurate facsimile of the original record. Therefore, managers should be aware that the choice of hardware is important when deciding on storage architecture and devices.



Photo: Keith Syvinski

While many regulations seek to be "technology neutral," that is, they don't specify which media may or may not be permissible, there are a number of U.S. and international laws and regulations that either specifically require or emphasize WORM technology (Write Once Read Many—an optical disk technology on which data can be written only once and thus become permanent) as the preferred technology for ensuring the trustworthiness of electronically stored records.

The United States Securities and Exchange Commission (SEC) regulation 17 CFR 240.17a-4(f) mandates that "the electronic storage media must: preserve the records exclusively in a non-rewriteable, non-erasable format."^[3] This regulation also stipulates that "if employing any electronic storage media other than Optical Disk technology, the member, broker, or dealer must notify its designated examining authority at least 90 days prior to employing such storage media." It should be noted there have been no reported instances of regulatory issues attributed directly or indirectly to the use of WORM storage subsystems or media over the many years that the technology has been in use by broker-dealers.

Record Retention

Most of a record's life cycle is spent being "stored." Therefore, the storage period is when records are vulnerable to intentional tampering or unintentional alteration or deletion. Unintentional tampering can happen during the process of migrating records multiple times due to storage media degradation or obsolescence over a long retention period. To the extent that a company in litigation can quickly dispose of any challenges related to the storage period by clearly showing that a record could not have been altered (short of a conspiracy involving technology experts and company insiders, or an incompetent or disgruntled employee^[4]), an expensive and time-consuming inquiry into record trustworthiness can thus be pre-empted.

Another growing concern of organizations is the risk of being cited for spoliation, the willful (or occasionally negligent) destruction of evidence that denies opposing parties their due rights. Courts in some jurisdictions allow mistaken and negligent conduct to form the basis of a claim for destruction of evidence. The potential for being cited for spoliation in litigation or a regulatory investigation is one of the greatest exposures corporations have under the stipulations of the Sarbanes-Oxley Act. Such a possibility puts a great burden on the storage mechanisms and applications being utilized to protect the records for the required retention period. Being cited for spoliation could result not only in severe sanctions and fines, but also in public embarrassment from exposure on the front pages of widely read financial and business newspapers and publications. Therefore, once again information systems' architecture choices necessitate a conversation between the CIO and legal counsel to ensure that proper systems are in place.

The challenge of ensuring record reliability grows in proportion to the length of time the electronic records must be retained. Retention periods can range from as little as three years to as long as fifty years or more, or in some cases, can be in perpetuity. Examples of industry segments and applications in which longer-term retention is required by regulation or good business practices include those in **Table 1**.

Table 1: Examples of Industry Segments in Which Longer-Term Retention is Required

Industry	Regulator	Record Type	Retention Period
Securities Broker/Dealers	SEC	New account records	Life of account + 6 years
Pharmaceutical	FDA	Records related to new drug applications	Date of submission + 5 years
Health Care	HIPAA*	Patient Records	Life of patient + "n"*** years
Government	FOI Act	Governmentally Created	20 to infinity years

*Health Insurance Portability and Accountability; ** Number of years

Readily Retrievable

From a regulatory perspective, records are typically expected to be "readily" accessible (within hours or at least on the same day) during the first two to three years of their required retention period, the period when the potential for a regulatory investigation or audit is highest. Thereafter, records should be retrievable within a reasonable period of time (typically days, not months). Legal discovery orders must also be satisfied within a specified period of time generally measured in weeks or months rather than hours or days.

From a business perspective, the frequency of and access speed for records retrieval is relatively high for new records. Retrieval time then decreases with the age of the record. In a number of situations, the retrieval activity of a record may be very low for many years. Then, based on the occurrence of a particular event such as the payoff of a mortgage loan or the payout of a life insurance policy, a spike of activity may occur.

When a record has reached its inactive or archival state and possibly has been moved to a slower, lower cost electronic records storage medium, a slower response time to retrieve the record would generally be considered understandable and acceptable by the courts and most regulators.

However, the integrity of the record must be protected for the full retention period in a manner that makes it retrievable, processable (using available hardware and software) and accurately reproducible in a form that is human-readable. This requirement puts significant pressure on a firm to have in place policies related to data archaeology and forensics and to make technology decisions accordingly.

Disaster Recovery

To ensure that records are truly readily retrievable, most regulations, as well as information systems best practices, require that a copy of fixed content or reference electronic records be kept at a separate

geographical location for purposes of disaster recovery. Disaster copies are most often written to, and retained on, removable media (e.g., CD-ROMS, tapes, and floppy drives) unless very high-speed access is required when the copies need to be restored. Removable media generally provide the most cost-effective solution for storing disaster copies because these copies rarely need to be accessed and restored, and off-line shelf storage is the lowest cost solution. Many organizations are opting to outsource their data recovery function as expense and complexity of such storage and retrieval increase.

Trustworthiness

Reliability of records is irrelevant if the data are not accurate and trustworthy in the first place. One way to ensure trustworthiness is to view the components related to storage of electronic records in the context of a "chain of trust." A number of potential components in an electronic records environment can be applied to protect the integrity of electronic records: the application, the logical file management system, the physical storage system, and the media. The more components that are employed to ensure that electronic records are not altered or deleted prior to their required retention period, the more likely the storage environment will be viewed and accepted as being trustworthy. This concept is extremely important in determining appropriate data and system architecture.

If any one link in the "chain of trust" is found to be weak by a court of law or a regulatory investigation, or if the record cannot be produced due to a weakness or failure of a component in that chain, then the overall process, procedures and system of storing all of an organization's electronic records could be challenged, and the record could be found inadmissible in evidence by the courts. In addition, if the record cannot be produced due to a weakness or failure of a component, then a fine, sanction, or even a judgment of spoliation could result.

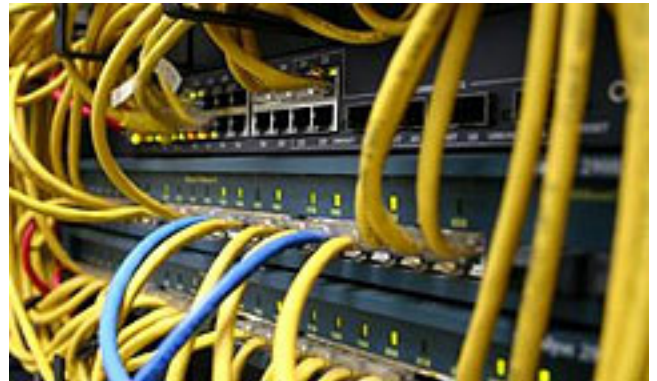


Photo: Craig Gault

Accuracy

Central to the notion of evidentiary trustworthiness and regulatory compliance is the need to ensure accuracy of data. This means that the record and all actions related to the record can be accounted for during its life. Sometimes this requirement is referred to as the "chain of custody"[5] or audit trail. An audit trail can be very useful as evidence to show that the records have been properly managed, thereby helping prove that no unauthorized alteration of the record or its associated metadata has occurred during the record's life. Such a trail lowers the risk that an alteration to a record could go unnoticed and makes it less likely that the record would be questioned, either in the course of litigation or in regulatory investigations.

Most audit trails are kept at an application level. However, some technology, such as WORM, does not allow deletion or alteration of records (or associated index information written to the media), thereby providing an inherent and automatic audit trail of all stored records. The decisions as to whether to implement an identity management system, a hard-token security system (which requires a physical "key" of some sort), workflow software, or just to ensure that there are certain points at which the data become permanent are all important options that managers must carefully consider when deciding about their data processes and architecture.

Summary

Because of the explosive growth of electronic records, the mandate for trustworthy storage and management of electronic records is greater than ever before. Compliance with new laws and regulations mandates records storage reliability, retention, ready retrievability, and accuracy, all of which in turn impact IT policy and choices. In this regard managers should be preparing organizations now in the following ways:

- Each user organization must have a solid and comprehensive plan for managing electronic records, including up-to-date retention schedules.
- Every application should be evaluated based on its requirements for protecting the integrity, accessibility and retention life of the electronic records being created, received, and stored.
- Industries and applications with higher risks for litigation or regulatory investigation (or both) must use extra diligence in establishing a chain of trust that inherently and obviously protects electronic records from alteration and premature deletion.

Charla Griffy-Brown, PhD, is an associate professor of Information Systems and Technology Management at Pepperdine University's Graziadio School. A former Fulbright Scholar, Dr. Griffy-Brown graduated from Harvard University, and holds a Ph.D. in Technology Management from Griffith University, Queensland, Australia. In 2004, she received a research award from the International Association for the Management of Technology, which recognized her as one of the most active and prolific researchers in the Technology Management and Innovation field. She has published widely in the area of technology management and information systems. charla.griffy-brown@pepperdine.edu

Stepheni Bodo, is a third-year student at the Graziadio School and has more than eight years of FDA computer systems quality and compliance experience working in the pharmaceutical, medical device, and biotech sectors. In addition, she has 15 years of information technology experience in research and development labs, the legal sector, and pharmaceutical R&D and manufacturing. In her role as principal consultant at 21 CFR Consulting, she leads her clients into an elevated state of regulatory compliance through proven validation techniques and offers her industry expert guidance to technology firms breaking into the regulated industry software sector.

Linnea Bernard McCord, JD, MBA, an associate professor of Business Law, received her Juris Doctor degree from the University of Houston Law Center, where she was an editor of the Law Review. She received her Master of Business Administration degree from the University of Texas at Austin, where she was the recipient of the George Kozmetsky award for academic excellence. Dr. McCord has spent more than 28 years practicing and teaching business law and business ethics in both academic and corporate environments and is a former General Counsel of a division of a Fortune 500 high-technology multinational company with headquarters in New York and Paris. linnea.mccord@pepperdine.edu

[1] Federal Rules of Evidence, Rule 803(6), 2004 Go to (<http://uscode.house.gov/search/criteria.php>) In the search box, type in "Federal Rules of Evidence Article VIII, Rule 803.

[2] Uniform Trade Secrets Act, 14 U.L.A. 189, 1990 (Go to <http://uscode.house.gov/search/criteria.php>) In the Search box, type in "Sec. 1732. Record made in regular course of business; photographic."

[3] Title 17- Commodity and Securities Exchanges Chapter II - Part 240 General Rules and Regulations, Subpart A - Rules and Regulations Under The Securities Exchange Act of 1934, Sec. 240.17a-4. Records to be Preserved by Certain Exchange Members, Brokers and Dealers.", Securities and Exchange Commission, 2004 (<http://www.sec.gov/rules/final/34-46473.htm#VIIIIB2>).

[4] "Surveys: Human Error Is the Culprit in Data Loss", Government Computer News Vol. 18, No. 29, Drew Robb, 09/06/1999 http://www.gcn.com/vol18_no29/enterprise/553-1.html.

[5] "California Civil Discovery Law: Discovery of Electronic Data", Richard E. Best, 1998.

The opinions expressed are those of the authors and do not necessarily reflect the views of the Graziadio School of Business and Management or Pepperdine University.