

Cohasset Associates, Inc.

White Paper

April 2003

Trustworthy Storage and Management
of Electronic Records

The Role of Optical Storage Technology

Cohasset Associates, Inc.

3806 Lake Point Tower
505 North Lake Shore Drive
Chicago, Illinois 60611

Tel. 312.527.1550

Table of Contents

<i>Introduction</i>	1
<i>Establishing Trustworthiness</i>	2
The Risk and Cost	3
<i>Challenges to Trustworthiness</i>	5
Durable Medium	6
Chain of Custody or Audit Trail	7
<i>Trustworthiness Over Time</i>	8
Accessibility Over Time	10
Storage Cost versus Access Performance	10
Disaster Recovery	12
Migration	13
<i>Electronic Records Chain of Trust</i>	14
<i>Summary</i>	15
<i>Appendix A. Legal and Regulatory Reference Material</i>	17
United States	17
International	18

Introduction

Companies and public entities must retain records for a variety of reasons:

- To comply with laws and regulations that mandate records retention,
- To retain the “corporate memory” of activities and events that may be required to meet ongoing business and historical needs, and
- To provide evidence in the event of an investigation or lawsuit in both regulated and non-regulated industries.

Increasingly, electronic records are defined in laws and regulations as being equal to traditional paper and micrographic records. This legal and regulatory evolution is recognition that the great majority of contemporary fixed content business and public records are now “born” electronic or converted to an electronic format. A second factor is that the volume of this fixed-content or “reference” information is growing at 50-80% or so per year – a growth that is well beyond the ability of an ever-expanding number of organizations to continue relying on manual intensive paper and micrographic formats as official records.

The majority of electronic fixed-content and reference records (like their non-electronic predecessors) must be retained in accordance with legal and regulatory requirements as well as for business needs. The risks of improper retention and management of records has grown substantially with the newly passed laws that embody penalties consisting of greater fines and jail terms such as is manifested in the Sarbanes-Oxley Act of 2002.

Private and public entities must understand and meet the formidable and critically important challenge of both understanding and operating in accordance with the applicable laws and regulations. To that end, they must reduce the legal, regulatory and business risks involved in the capture, storage, management and reproduction of their electronic records.

The legal and regulatory acceptance of electronic records is predicated on these records meeting certain well established requirements. The overriding requirement is that they are authentic and can be deemed to be accurate, reliable and trustworthy.

Optical disk storage, like all forms of digital storage has a very important role in establishing and maintaining the accuracy, reliability and trustworthiness of electronic records. To date, optical disk storage has achieved this without any known legal exceptions. The durability, robustness, removeability, longevity (including backward read compatibility) and flexibility of access (in near-line, off-line and selected on-line applications) suggest that optical disk storage will continue to play an important role for storing electronic records in a trustworthy manner.

This purpose of this White Paper is to examine the role of digital optical storage as it relates to establishing and maintaining the trustworthiness of electronic records. The focus of this paper is on cartridge-based, 5¼ inch write-once, read-many (WORM) optical disk storage that is used in

mainstream commercial and public sector applications, which produce electronic records. DVD and CD technologies, because they are most often used for consumer or personal storage purposes, are not included in scope of this paper.

Cohasset Associates, Inc. was commissioned to produce this White Paper by a coalition of companies that market digital optical storage products. The sponsoring companies were: DISC, Hewlett Packard, Plasmon, and Sony Electronics. Only publicly available information was used in Cohasset's research. The information, analyses and conclusions presented in this White Paper were independently derived by Cohasset. They were not influenced by nor did they result from information provide by the sponsors.

Cohasset is widely recognized as one of the nation's foremost management consultants specializing in electronic records management. Over the past three decades, Cohasset has served more than 300 clients. For nearly twenty-five years Cohasset has been recognized for its authoritative and incisive work in the legality of alternative media. This included editing of the definitive legal research study, *Legality of Optical Storage* (<http://www.cohasset.com>).

Establishing Trustworthiness

In the statutes and regulations of the United States, Canada, Europe, Australia and other nations that have promulgated electronic record legislation, there is a common set of foundational requirements regarding the acceptance of electronic records in a court of law or regulatory hearing:

- The records must be authentic – i.e. there should be proof that “they are what they purport to be”,
- The integrity of the records must be protected from alteration or deletion for as long as the records are retained,
- The records must be “readily” accessible whenever they may need to be retrieved,
- When retrieved, the records must be capable of being processed (by available hardware and software) and reproduced in a format that can be read by a person;
- In selected regulations, and in all good practices related to electronic records storage, a duplicate “recovery” copy of the original electronic record is required and it must be kept at a separate geographical location, and
- In accordance with good recordkeeping practices, an increasing number of laws and regulations require an audit trail (i.e., the process and management evidence) be produced and retained as a means of tracking any possible alterations to the record (and its associated metadata), as well as other events such as the migration of the record, e.g., the transfer of records from one media to another.

What trustworthiness attributes of an electronic record will be considered when establishing the authenticity and intrinsic credibility of an electronic record in: 1) a court of law, 2) a regulatory investigation, or 3) any organization that may serve as an adjudicator, recipient or keeper of electronic records?

- The electronic record was captured at or near the time of the event or transaction¹,
- The electronic record has been relied upon in the normal course of business – i.e., the processes and equipment used to create and retain the record are reliable and can be trusted,
- The original content, the context and the structure of the electronic record have been preserved for the full retention life of the record – including any migration of the record from one system or medium to another,
- The electronic record is accurate and complete, i.e., the integrity of the record has been maintained, for the full retention life of the record – from the point when it was created or received and stored until final disposition at the end of any required retention period, and
- The electronic record is available for retrieval as requested for legal, regulatory or business purposes – under both normal business circumstances and in the event of a disaster.

The Risk and Cost

The risk and cost of not retaining records in a trustworthy and readily accessible manner can be substantial, as shown by these relatively recent examples:

- A major company was fined \$1,000,000 by the court, which found repetitive instances where employees had destroyed records in defiance of a court ordered Records Hold relating to current litigation.
- Five Wall Street brokerage firms were fined a total of \$8,250,000 because they had “inadequate procedures and systems to retain and make accessible e-mail communications.”
- Arthur Andersen & Company literally “paid with its life” for the illegal destruction of records — both paper and electronic – in the face of a pending regulatory investigation.

When a record is offered as evidence in any formal legal or regulatory proceeding, it needs to be able to pass two tests:

1. Admissibility – should the record be admitted as evidence into the proceeding at hand, and
2. Credibility – is the weight ascribed to the record’s contents by the respective parties in a litigation or regulatory investigation.

Thus, even if a record meets the test of admissibility in evidence, the content and context of the record, as well as the process by which the record was stored and managed, can be challenged in the course of a legal or regulatory proceeding.

The greater the risk that an organization might be subjected to litigation or to a regulatory investigation, the more important it is to ensure that the organization's records have been stored, managed and preserved with the highest degree of trustworthiness – from the time they were created or received until final disposition.

Examples of industries with a high risk for litigation:

- Securities
- Insurance
- Healthcare providers
- Consumer product manufacturers (toys, household appliances, etc.)
- Construction materials
- Food manufacturers
- Automobiles, parts and tires
- Pharmaceutical and device manufacturers

Examples of industries with a high risk for regulatory investigation (parentheses indicate the applicable regulatory agency):

- Securities firms (SEC)
- Food manufacturers (FDA)
- Healthcare services (HIPPA)
- Insurance (State Insurance Commissioners)
- Pharmaceutical and device manufacturers (FDA)
- Utilities - non-nuclear and nuclear (FERC and AEC)

Certain businesses, such as large financial service and insurance companies, have exceptionally high volumes of electronic records. Accordingly, there are much larger numbers of records at risk if the integrity of the record is not fully protected. Also, greater quantities of records add to the challenge of accessing needed records promptly.

The industry segments and applications that appear on these lists and particularly those that appear on both, have the greatest legal and regulatory risk. They therefore have a greater need for ensuring that the integrity of their records has been well protected for the required retention period, and that they can be made retrieved within a reasonable period of time as required by regulatory agencies or the courts.

A Trial within a Trial

The use of new technologies to manage electronic records has the potential to create a “trial within a trial”. This normally occurs in a situation where the accuracy of the process used to create, store, protect and retrieve the record and, therefore, the reliability of the records is put into question. In such situations, the technology used to manage the records can be raised as a major issue related to its authenticity or trustworthiness. This issue may need to be resolved via court rulings – the trial within a trial – that can be time-consuming and distracting to the focus of the primary trial.

Depending on their scope and the technical detail required to address the issues, they also can be costly. While there is no precise measure of the hard costs that could be associated within a trial within a trial, there are several potential component costs that can be identified. They include, but are not limited to: expert witness fees, additional lawyers' fees, deposition costs and travel expenses. Additionally, in certain circumstances, a court can compel the losing party (on this issue) to reimburse the prevailing party for reasonable expenses.

Good records management can virtually eliminate the possibility of a trial within a trial by having processes, practices and storage management solutions that can be shown to be inherently and obviously trustworthy over the then-current life of the record. The risk and cost of a trial within a trial can be greatly reduced or even eliminated if it can easily be demonstrated that the electronic records in question, by virtue of the process and means used to store them, could not have been altered at any time after they had been committed to storage.

Challenges to Trustworthiness

An attack on specific electronic records also can include an attack on the process by which they were managed, including their creation, retention, reproduction or migration. The fewer weaknesses found in the storage and management of the record over its lifecycle, the greater the likelihood that the record will withstand any legal challenges regarding its admissibility and, most importantly, its credibility. This is true not only in litigation, but also in regulatory audits and investigations.

There are four potential weaknesses where the process of managing electronic records could be challenged:

- A storage medium or subsystem that is inherently or potentially alterable;
- The risk of records being lost or altered when the storage solution or media required frequent migrations resulting from technology degradation or obsolescence over the course of a long retention period;
- Little or no documented evidence (audit trail or chain of custody) of the events that have occurred over the record's lifecycle; and
- Insufficient protection of the record from alteration or deletion in the processes, procedures, systems, storage solutions, or storage medium utilized.

Most of a record's lifecycle is spent being "stored." Therefore, this is the longest period of time where records are vulnerable to intentional tampering or unintentional alteration or deletion – such as during the process of migrating records multiple times due to storage media degradation or obsolescence over a longer retention period.

To the extent that a party in litigation can quickly dispose of any challenges related to the storage period by clearly showing that a record could not be altered (short of a conspiracy involving

technology experts and company insiders or an incompetent or disgruntled employee.ⁱⁱ), an expensive and time-consuming inquiry into record trustworthiness can be preempted. Further, using a storage medium that reduces or eliminates the need for migration of the records during the full retention period reduces the risk that the integrity of the electronic record would be challenged.

Another growing concern of organizations is the risk of being cited for spoliation, which is the willful (or occasionally negligent) destruction of evidence that denies an opposing party their due rights. Courts in some jurisdictions allow mere mistaken and negligent conduct to form the basis of a claim for destruction of evidence. The potential of being cited for spoliation in litigation or a regulatory investigation is one of the greatest exposures to corporations under the requirements of the Sarbanes-Oxley Act. This trend is particularly problematic and puts a much greater burden on the storage mechanisms and applications being utilized to protect the records for the required retention period. Being cited for spoliation could not only result in severe sanctions and fines, but also public embarrassment from exposure on the front pages of widely read financial and business newspapers and publications.

Durable Medium

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” (emphasis added)ⁱⁱⁱ. With the advent of electronic records, the interpretation of a “durable medium” has expanded to encompass electronic storage media. This statute sets forth certain fundamental requirements that must be satisfied in order for a reproduction of an electronic record to be as acceptable as the original. Specifically, it states that the medium used for the storage of records must be reliable and exhibit attributes that supports the reproduction of an accurate facsimile of the original record.

While many regulations seek to be “technology neutral” in that they may define a “system of controls” to ensure the trustworthiness of records, there are a number of U.S. and international laws and regulations that either specifically require or emphasize optical disk technology as the preferred medium for ensuring the trustworthiness of electronically stored records:

- The United States Securities and Exchange Commission 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.*” This regulation also stipulates: “*If electronic storage media is used by a member, broker, or dealer it shall comply with the following requirements: ... If employing any electronic storage media other than Optical Disk technology, the member, broker, dealer must notify its designated examining authority at least 90 days prior to employing such storage media.*”^{iv} It should be noted there have been no reported instances of regulatory issues attributed directly or indirectly to the use of WORM optical disk storage subsystems or media over the many years that the technology has been in use by broker-dealers.
- The Australian Evidence Act abolishes the “original document rules” which “requires the production of the original document in writing.” The law states that one of the acceptable alternative ways to offer evidence includes “*a printout of computer output or a document reproducing the contents of an optical laser disk*” (emphasis added).

- The French standard, NF Z 42-013 requires that only WORM media, as defined in section 3.7 of that standard, may be used for the storage of electronic documents that are to be admitted as evidence in a court of law. Section 3.7 defines WORM media as “optical medium in which the bits coding the data are written by a non-reversible transformation of one or more components of the medium.”

The continued requirement or emphasis by certain laws and regulations that WORM digital storage, and specifically optical disk technology, be utilized to protect the integrity and reliability of electronic records suggests that WORM optical technology is still viewed by selected lawmakers and regulators as providing certain beneficial characteristics, such as non-erasability and durability, that enhance the trustworthiness of electronic records. See Appendix A for additional legal and regulatory reference material and details.

Chain of Custody or Audit Trail

Central to the notion of evidentiary trustworthiness and regulatory compliance is that the record, and all actions related to the record, can be accounted for during its life – sometimes this is referred to as the “chain of custody.” An audit trail can be very useful as evidence to show that the records have been properly managed, thereby helping “prove the negative”, i.e., that no unauthorized alteration of the record and its associated metadata has occurred during its life. Simply put, this lowers the risk that an alteration to a record could go unnoticed and, therefore, 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, the use of WORM optical disk technology that is durable and does not allow deletion or alteration of records (or associated index information written to the media) provides an inherent and automatic audit trail of all stored records, short of any willful or accidental defacing or destruction of the media.

Trustworthiness Over Time

The challenge of ensuring trustworthiness grows in proportion to the length of time the electronic records must be retained. Retention periods can range from as little as three years up to fifty years or longer and, in some cases, permanently. There are a number of regulatory and business environments that require records to be retained for extended periods of time. Examples of industry segments and applications where longer term retention is required by regulation or good business practices are:

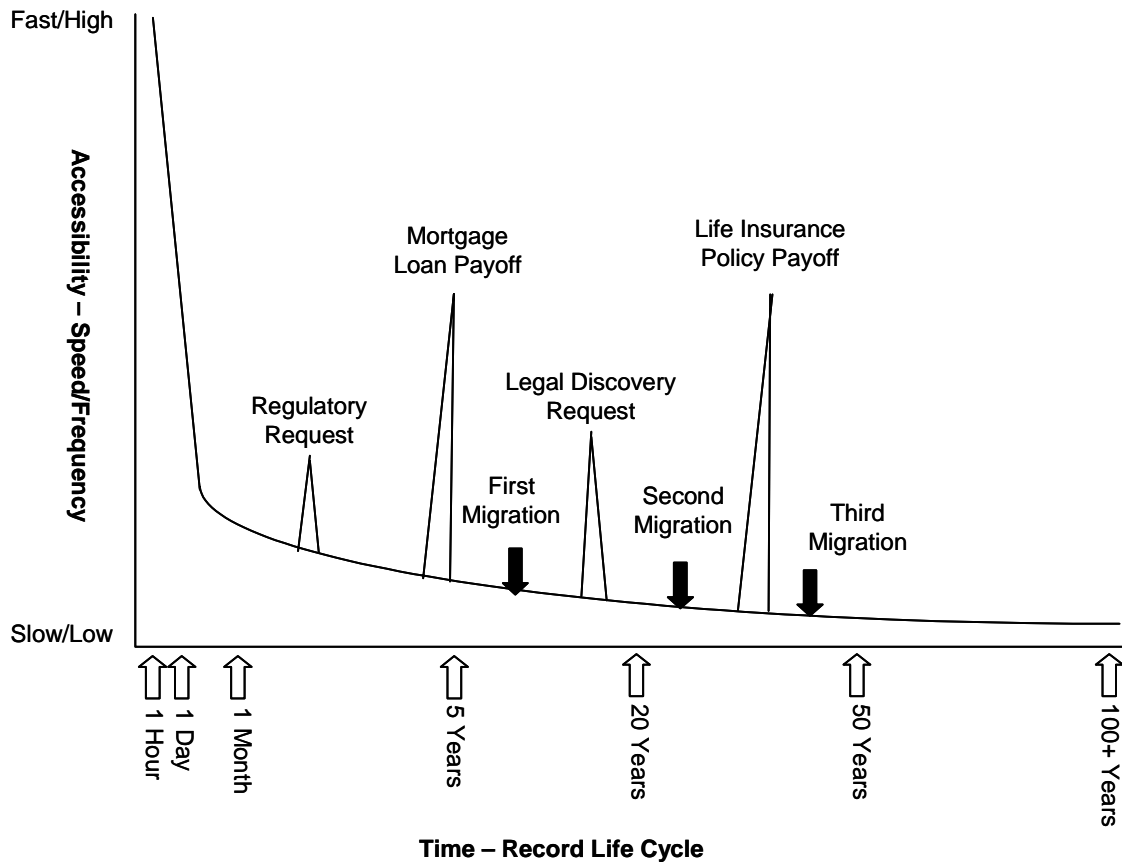
Industry Segment, Regulator and Type of Record	Typical Retention Period
Securities broker/dealers: new account records	Life of account plus 6 years
Pharmaceutical: FDA Good Laboratory Practices; records related to a new drug applications (NDAs)	Date of submission plus 5 years
Life Insurance: policy information	Life of policy plus 6-10 years
Financial Services: mortgage loan files	Life of loan plus 6-10 years
Health Care: medical records	Life of patient plus “n” years
Government records	Many have a longer life (20-50 years, including permanent*)
Copyright records (all organizations)	Life of copyright = 95 years or as business needs dictate
Employee records (all organizations)	Termination plus 6-10 years
Employee medical records (all organizations)	Termination plus 30 years
General contract records (all organizations)	Life of contract plus 6-10 years
Utility (non-nuclear); FERC; plant records	Plant retirement plus 10 years

* Records transferred to the National Archives and Records Administration (NARA)

Certain regulated records have relatively short retention periods, unless they are extended due to litigation or regulatory actions. Two examples are 1) specific marketing and transaction records in the securities industry that have a three to six year retention period, and 2) tax records which have a seven year retention period.

Figure 1 depicts the life cycle of an electronic record, as a function of access frequency and speed, relative to the life cycle of an electronic record – which could range from a few years up to 20 or 50 years or even permanent

Figure 1. Records Life Cycle vs. Accessibility



Migration of Records

A major issue for electronic records with longer retention periods (typically ten years or longer) is the need to “migrate” the records periodically due to system or media obsolescence. This copying between media technologies or transferring of electronic records between systems can be very costly and time consuming and may increase the risk of inadvertent loss or alteration.

The following are considerations for potentially reducing the need for frequent migrations:

- *Greater backward read compatibility* – when the media from one generation of a base technology can be read by the next or multiple future generations. The more generations of a base media technology that can support backward compatibility of older generations, the less likely a media migration will need to be undertaken.

Optical disk technology, particularly the 5¼ inch cartridge-based media, has been able to provide backward compatibility for four to five generations. However, one can seldom expect the period between migrations to be longer than 15-20 years due to obsolescence of supporting hardware/software system and applications. Using optical disk technology to store records with a retention period of 15-20 years or longer may reduce or eliminate the need for electronic records to be migrated, thereby reducing or eliminating the risk of alteration or loss during migration, and saving the cost and resources involved.

- *Longer useful media life:* the media life expectancy should be at least as long as the period of time until the first media migration is required. Optical disk technology, due to its durable composition and construction, has a predicted life expectancy of 30 to 50 years and longer, which can readily support an initial migration frequency of 15-20 years. Magnetic media technology, especially magnetic tape, may require more frequent migrations depending on the degree to which specified environmental controls are maintained and how frequently technology upgrades are required.

Accessibility Over Time

Retaining records for longer periods of time can raise important questions about the frequency and speed with which records can be accessed. The time period within which different types of electronic records must be made accessible varies according to the requestor, the nature of the request and the age of the records being requested:

- From a regulatory perspective, records are typically expected to be “readily” accessible (within hours or latest 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, regulators will expect records to be retrievable within a reasonable period of time (typically days and not months).
- Legal discovery orders must also be satisfied within a specified period of time, which generally is measured in weeks or months rather than hours or days.
- From a business perspective, the frequency of and access speed for records retrieval generally starts relatively high, and 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, there will be a spike of activity – as noted in Figure 1.
- When a record has reached its inactive or archival state and possibly has been moved to a slower, lower cost electronic records storage medium, such as to near-line or off-line optical disk storage, a slower response time to retrieve the record would generally be considered understandable and acceptable by the courts and most regulators.

Independent of access activity or age, the integrity of the record must be protected for the full retention period in a manner that makes it retrievable, processible (using available hardware and software) and accurately reproducible in a form that is human-readable.

Storage Cost versus Access Performance

The diagram in Figure 2 details the three types of storage that are normally considered for electronic records, depending on the speed and frequency of access. They are:

- **On-line and Near-on-line:** On-line storage is generally provided by magnetic disk. It is used in the very active stages of an electronic records life – when it is being created or received and processed, as well as when the access frequency is high and the required speed of access is very fast, i.e., in milliseconds.

Near-on-line is a more recent category of relatively high speed (1 or 2 second access speed) storage and generally is lower cost than on-line storage. In selected applications, where records may not require frequent or high speed access, such as for certain reference-type records, near-line optical disk technology may satisfy the need.

- **Near-line:** This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple write/read devices to store and retrieve records. Access speeds can range from as low as milliseconds if the media is already in a read device, up to 10 - 30 seconds for optical disk technology, and between 20 - 120 seconds for sequentially searched media, such as magnetic tape. Near-line storage provides a reasonable speed-of-access to records, generally at a lower cost than on-line or near-on-line storage.

Optical disk technology, particularly the cartridge-based, 5¼ inch technology, is the most frequently used media for near-line storage of electronic records, primarily because it provides a durable and robust media for robotic handling and offers the fastest access speed of the removable media technologies.

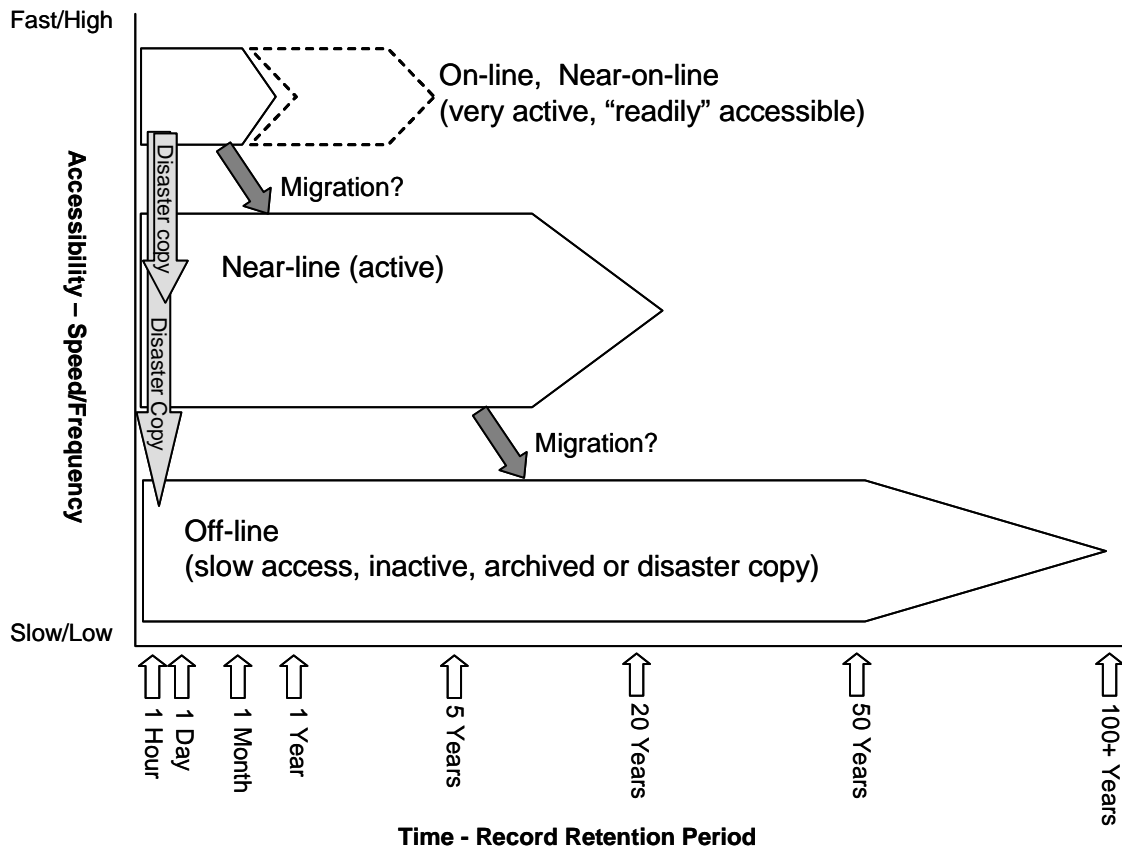
- **Off-line:** This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered “archival” in that their likelihood of retrieval is minimal. Accessibility to off-line media involves manual intervention and is much slower than on-line or near line storage. Access speeds may be minutes, hours or even days, depending on the access-effectiveness of the storage facility.

Electronic records stored in near-line robotic libraries are prime candidates for being moved off-line when they become inactive or can be archived. When later needed, the records then can be reloaded into the robotic library.

The records storage capacity for all types of digital storage media continues to rapidly increase. This results in an equally rapid decrease in the cost for each electronic record stored. A new generation of cartridge-based, 5¼ inch optical drives and media based on “blue laser” technology will begin production deliveries in 2003. The initial generation of advanced blue laser technology will provide almost triple the storage capacity of currently available optical media^{vi}. Initial media capacities for blue laser technology will range from 23 to 30 gigabytes per cartridge in the first generation, growing to 120 GB per cartridge in the future. This in turn will result in proportional capacity increases in robotic library configurations.

A thorough evaluation of capacity, access performance and cost requirements should be performed by users for every application in order to determine the most effective cost/performance method for storing, retrieving and managing records.

Figure 2. Record Accessibility Over Time



In applications or organizations, such as a small to medium entities, where capture volumes and the frequency and speed of access may not be as high or demanding, the use of near-line or off-line storage – such as cartridge-based 5¼ inch optical storage technology – may satisfy both the business as well as the legal and regulatory accessibility requirements. It also may prove to be a more cost effective solution, particularly as the blue laser technology media becomes available.

Disaster Recovery

Most regulations, as well as good records management and good information systems practices require that a copy of fixed content or reference electronic records be kept at a separate geographical location for purposes of disaster recovery. A disaster copy of a record is different from a traditional “backup copy” in that the disaster recovery copy is never intended to be overwritten^{vii}. To ensure the effective recovery of records, the disaster recovery copy should be made at or near the time when the original record is written to storage – as noted by the “Disaster Copy” arrows in Figure 2.

Disaster copies are most often written to and retained on removable media, unless very high speed access is required when the copies need to be restored. Removable media generally provides the most cost-effective solution for storing disaster copies because they rarely ever need to be accessed and restored, and off-line shelf storage is the lowest cost solution. A durable media

like cartridge-based, 5¼ inch optical media, which has a long shelf life and a history of successfully providing backward read compatibility across multiple generations, is particularly well suited for storing disaster copies, especially for records that have a longer retention period (8-10 years or more).

Migration

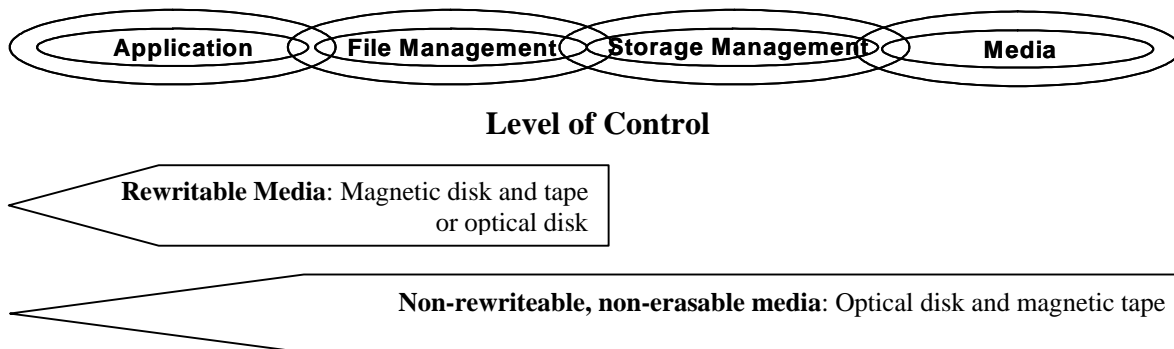
As noted in the section on Trustworthiness Over Time and as indicated in Figure 1 and Figure 2, records with a long retention period (particularly 10-20 years and longer) may require migration due to the obsolescence of: a) the media, b) the write/read devices, or c) the supporting application software or hardware. Cartridge-based 5¼ inch optical media, which provide multiple generations of backward read compatibility and a media shelf life of 30-50 years and longer, are particularly well suited for reducing or even eliminating the number of migrations that may be needed over a longer retention period. Accordingly, this could reduce or eliminate the risk of records being altered or lost during multiple migrations.

Another reason for migrating or copying records from on-line or near-on-line storage (as indicated by the arrows in Figure 2 labeled "Migration?") is to lower the overall cost of storage relative to the accessibility requirements. As the access speed and frequency requirements for certain electronic records decrease over time, consideration could be given to migrating them to a slower, lower cost near-line or off-line storage solution. Cartridge-based 5¼ inch optical disk technology provides the removeability features that meet these requirements. In this context, optical disk technology can be viewed as providing a complementary alternative to on-line or near-on-line magnetic storage.

Electronic Records Chain of Trust

One way to view the components related to trustworthy storage of electronic records is in the context of a “chain of trust” The chain of trust graphic depicted in Figure 2 indicates that there are a number of potential components in an electronic records environment that can be applied to protect the integrity of electronic records: a) the application, b) the logical file management system, c) the physical storage system, and finally d) the media.

Figure 3. Electronic Records Chain of Trust



Functions	Functions	Functions	Functions
<ul style="list-style-type: none"> • Creates or receives record and manages record disposition* 	<ul style="list-style-type: none"> • Manages logical write/read and access to records. 	<ul style="list-style-type: none"> • Manages physical write/read and access to records. 	<ul style="list-style-type: none"> • Physical storage of records.
Components	Components	Components	Components
<ul style="list-style-type: none"> • Prepare record for writing • Initiates search and retrieval 	<ul style="list-style-type: none"> • File directory • File attributes • Executes retrieval 	<ul style="list-style-type: none"> • Write/read device • Device controller • Robotic library 	<ul style="list-style-type: none"> • Media
Controls	Controls	Controls	Controls
<ul style="list-style-type: none"> ▪ Writes record ▪ Version control ▪ Audit trail ▪ Access metadata ▪ Access security - role/function ▪ Manages disposition (retention metadata)* 	<ul style="list-style-type: none"> ▪ Overwrite protection (read only, other) ▪ Write verification (hash/checksum) ▪ Validate integrity at retrieval time and/or periodically (hash/checksum) ▪ Retention protection 	<ul style="list-style-type: none"> ▪ Write once (detecting read-only media) ▪ Write verification (hash/checksum) ▪ Robotics and caching for ready accessibility 	<ul style="list-style-type: none"> ▪ Non-rewriteable, non-erasable (WORM)media

* Record disposition may be managed by another application (e.g., a recordkeeping system) either integrated with or separate from the creation/receipt application.

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.

As noted in Figure 3, there is a difference in the degree of protection that can be provided between erasable and non-erasable media:

- Erasable and rewritable magnetic or optical media can only be protected to the level of logical file management – plus any protection offered by the application – because the storage management (library, controller/drive) and media do not inherently provide protection.
- Non-rewritable, non-erasable media, such as cartridge-based WORM 5¼ inch optical technology, offers protection starting with the physical media and storage management components. This protection would be further enhanced through any additional controls provided by the file management system and the application.

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, then:

- The overall process, procedures and system of storing all of an organization’s electronic records could be challenged by the courts or a regulatory authority;
- The record could be found as inadmissible in evidence by the courts; or
- 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.

Summary

Laws and regulations stipulate one or more of the following three methods for protecting the integrity of records:

- Establishment of a basic set of requirements that must be met for the full retention period of the record:
 - The integrity of the record must be protected;
 - Accessibility to the records must be provided; and,
 - In some instances, an audit trail of events related to the record must be kept;
- Delineation of a system of controls that are designed to protect a record’s integrity as well as provide accessibility and accountability (audit trail) for the full retention period; and

- Employ a media technology that inherently protects against alteration and deletion, e.g., non-rewriteable and non-erasable or WORM.

Cartridge-based, 5¼ inch WORM optical disk technology provides an important set of attributes that support the requirements established by these laws and regulations, as well as supporting overall good practices for managing electronic records:

- ***A durable medium*** – designed to be relatively impervious to environmental contaminants and housed in a robust, fully encased cartridge.
- ***Non-rewriteable and non-erasable storage*** – offering protection of the electronic record at the lowest level of the chain of trust – the media and storage management components.
- ***Removeability*** – offering solutions for inactive, archival and, in certain cases, active access requirements, and making it particularly well suited for creating and retaining disaster copies of electronic records.
- ***Media longevity*** – the longest shelf life of any digital media.
- ***Backward read compatibility*** – a history of successfully providing the ability to read older media generations with newer write/read drive generations. In turn, this potentially reduces the number of migrations which then reduces the risk of record alteration or loss.

Due to the explosive growth of electronic records, the mandate for trustworthy storage and management of electronic records is greater than ever before.

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 be extra diligent in establishing a chain of trust that inherently and obviously protects electronic records from alteration and premature deletion.

While there will undoubtedly be an increasing number of application, file management and digital storage solutions offered in the quest to address the explosive growth and expanding requirements for managing electronic fixed-content and reference records, cartridge-based, 5¼ inch WORM optical disk storage will continue to play an important role in establishing a storage environment that is accurate, reliable and trustworthy.

Appendix A. Legal and Regulatory Reference Material

United States

Legal

The Federal and State Rules of Evidence and Civil Procedure establish the foundation for admitting reproductions of electronic records (or copies of records) into evidence as if they were originals. The recent passage of the Electronic Signatures in National and Global E-Commerce Act (E-Sign) at the Federal level and the Uniform Electronic Transactions Act in various states make clear that electronic records have equivalent legal status relative to their paper equivalent, and that they can be retained as the “official record copy” or “official business record” for most commercial and public business purposes.

The “laws of evidence” is the system of rules and standards that regulates the admission of proof in a legal proceeding or at an administrative hearing.^{viii} The applicable rules of evidence depend on whether the legal proceeding is in federal court,^{ix} in state court,^x or before a federal^{xi} or state regulatory agency^{xii} The underlying objectives of rules of evidence are similar, however, regardless of the forum: Evidence that is relevant and can be proven to be “what it purports to be^{xiii}” would normally be admitted before the judge or jury, and evidence that is not should be excluded.

Generally, business records may be authenticated by the testimony of someone familiar with the records, such as a custodian or supervisor, that the document is, in fact, a record of the business.^{xiv} However, digitally stored records can be authenticated as a “data compilation”^{xv} or as the output of “a process or system used to produce an accurate result.”^{xvi}

The Uniform Photographic Copies of Business and Public Records as Evidence Act (UPA),^{xvii} which has been adopted by many states, seems to allow the introduction of records stored on digital media into evidence as originals.^{xviii} The UPA 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.” (Emphasis added)^{xix} Since WORM optical media would be considered a durable medium from which the original can be reproduced, optically stored documents should be admissible as originals.

Many states have amended their evidentiary statutes or enacted new statutes to specifically cover digitally stored records.^{xx} For example, New York enacted a new subdivision to apply to digitally stored records: CPLR § 4539(b) provides that

[a] reproduction created by any process which stores an image of any writing . . . which does not permit additions, deletions, or changes without leaving a record

of such additions, deletions, or changes, when authenticated by competent testimony or affidavit which shall include the manner by which tampering or degradation of the reproduction is prevented, shall be as admissible in evidence as the original.^{xxi}

As WORM optical storage does not permit deletions or changes, it is covered by the New York statute. Many other states have adopted statutes that explicitly provide that optically stored records will be admissible as “originals” with respect to the best evidence rule.^{xxii} A handful of states have enacted statutes that treat reproductions of documents stored optically as “duplicates.”^{xxiii}

Regulations

The federal and state governments appear to be hesitant to mandate the use of any specific technology because: 1) technology changes rapidly; and 2) it may induce unintended preference for one company’s product over another.

SEC Regulation 17 CFR 240.17a-4(f) which deals with e-records and record retention generally mandates that “the electronic storage media must: preserve the records exclusively in a non-rewriteable, non-erasable format.” Another of the SEC Regulation Sections indicates “If electronic storage media is used by a member, broker, or dealer it shall comply with the following requirements: ... If employing any electronic storage media other than Optical Disk technology, the member, broker, dealer must notify its designated examining authority at least 90 days prior to employing such storage media.”^{xxiv}

International

Without addressing individual jurisdictions, the evidentiary considerations in the other developed countries are typically similar to the United States. Various countries have been aggressive in their recognition of e-records. Canada, Australia and Great Britain have all sought to promote the legal acceptance of e-records provided they are trustworthy and authentic. Two examples:

- The Canadian Uniform Electronic Evidence Act states that, “*in any legal proceeding, the best evidence rule is satisfied in respect of an electronic record on proof of the integrity of the electronic record system in or by which the data was recorded or preserved.*”
- The Australian Evidence Act abolishes the “original document rules” which “requires the production of the original document in writing.” The new law states that one of the acceptable alternative ways to offer evidence includes “*a printout of computer output or a document reproducing the contents of an **optical laser disk***” (emphasis added).

ⁱ Rule 803(6) of the Federal Rules of Evidence, a “[r]ecord of a regularly conducted activity” such as a “memorandum, report, record, or data compilation, in any form” will be admissible if the record was made at or near the time by, or from information transmitted by, a person with knowledge, . . . kept in the course

of a regularly conducted business activity, and [made as part of] . . . the regular practice of that business . . .”

ⁱⁱ A recent survey entitled; “Human Error is Culprit in Data Loss” indicates that “users themselves damage three times more data than do viruses, floods, lightning, earthquakes and hurricanes combined.”

ⁱⁱⁱ 14 U.L.A. 189 (West 1990).

^{iv} Presumably, the Regulation mandates notice to its regulators to allow them the opportunity to determine their acceptance or rejection of the chosen storage media and process. While the Regulation does not advance a particular media, the fact that WORM optical disk does not require a waiting period once the notification has been filed indicates a potentially greater sense of inherent trust.

^v Chain of Custody can also be shown by a computerized audit trail, capturing meta-data to show who created it, who edited it, when it was modified, etc. However, use of computerized meta-data to show trustworthiness may be costly and time consuming.

^{vi} Blue laser optical technology is a professional 5.25 inch storage solution and the natural successor to 5.25 inch Magneto Optical (MO) drives and media. The use of blue laser technology provides much greater data densities resulting in dramatically higher media capacities and a renewed multiple-generation roadmap for professional 5.25 inch optical storage. First generation blue laser products have a 23GB-30GB capacity range and are expected to reach as high as 120GB in the future. Blue laser optical employs phase change recording and is available in both rewritable and write once (WORM) media formats. With its multifunction capabilities, dramatic increase in capacity and the decrease in cost per GB, blue laser optical technology clearly enhances and extends the role optical disk technology will play in many commercial and government applications.

^{vii} Backup media are typically recycled since they contain snapshot copies of information that is constantly changing, whereas disaster copies are defined as containing final or official content that is fixed and must not be overwritten during the required retention period.

^{viii} 1 Strong, John W., ed., McCormick on Evidence § 1, at 2 (4th ed. 1992) [hereinafter cited as McCormick].

^{ix} In federal courts, most evidentiary questions are resolved by application of the Federal Rules of Evidence (FRE), specially enacted statutes such as the Federal Business Records Act (FBRA), 28 U.S.C. 1732(a) (1970), and the myriad court decisions in which these evidentiary rules have been interpreted. For a more in-depth review of the FBRA, see Legality of Optical Records, at 5-15, 5-18.

^x State laws of evidence may be found in the “common law” (court decisions), special statutes, or rules of evidence adopted by the highest court in the state or passed by its legislature. In many states, the common law rules of evidence have been superseded by adoption of the Uniform Rules of Evidence (URE), which are substantially similar to the FRE. See, generally Unif. R. Evid., 13A U.L.A. 5 (West 1994). For a detailed discussion of the adoption of the URE, see Legality of Optical Storage, supra note 5, at 5-8. Instead of adopting the URE, several states have passed special statutes concerning the admissibility of business records and reproductions, such as the Uniform Business Records as Evidence Act (UBREA) and the Uniform Photographic Copies of Business and Public Records Act (UPA). However, the national trend among jurisdictions is toward adoption of the URE and FRE and repeal of these older uniform laws. For more discussion, see Legality of Optical Storage, supra note 5, at 5-8.

^{xi} Unlike the federal courts, federal administrative agencies are not bound by the Federal Rules of Evidence. 2 Davis, Administrative Law Treatise, § 10.1, at 117-18 (3d ed.1994). Instead, they must comply with the Administrative Procedure Act, which provides that “[a]ny oral or documentary evidence may be received, but the agency as a matter of policy shall provide for the exclusion of irrelevant, immaterial, or unduly repetitious evidence.” 5 U.S.C. § 556(d) (1996). This Act permits administrative agencies greater latitude in determining what evidence is admissible in their hearings than would be possible if the FRE were strictly applied. Essentially, some of the questions regarding accuracy, reliability and trustworthiness go to the “weight” of the evidence, rather than its admissibility. For more discussion, see Legality of Optical Storage, supra note 5, at 5-8, 5-14.

^{xii} Like their federal counterparts, the admissibility of evidence in a state agency proceeding will be governed by the applicable state administrative procedure act and the agency rules of practice and procedure.

^{xiii} See Fed. R. Evid. 901(a).

^{xiv} 2 McCormick, supra note 6, §219, at 688.

^{xv} Fed. R. Evid. 901(b)(8).

^{xvi} Fed. R. Evid. 901(b)(9).

^{xvii} 14 U.L.A. 185 (West 1990).

^{xviii} See, e.g., Mass. Ann. Laws ch. 233, §79E (Law. Co-op. 1998); S.C. Code Ann. § 19-5-610 (Law. Co-op. 1997); Vt. Stat. Ann. tit. 12, § 1701 (1998). Similarly, an Oregon statute, which states that “[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original,’” seems to cover data stored on an optical disk. Or. Rev. Stat. § 40.550 (1997). See also Iowa Code § 622.28 (1997).

^{xix} 14 U.L.A. 189 (West 1990).

^{xx} See Kennedy and Thomas, supra note 5, at S3.

^{xxi} N.Y. C.P.L.R. § 4539(b) (McKinney 1998).

^{xxii} The following statutes apply to business records and public records: Ark. Code Ann. § 16-46-101 (Michie 1997); Colo. Rev. Stat. § 13-26-102 (1997); Ga. Code Ann. § 24-5-26 (1998); Ill. Comp. Stat. Ann. 5/115-5 (West 1998); Kan. Stat. Ann. § 60-469 (1997); Me. Rev. Stat. Ann. tit. 16, § 456 (West 1997); Md. Code Ann., Cts. & Jud. Proc. § 10-102 (1997); Minn. Stat. § 600.135 (1997); Neb. Rev. Stat. Ann. § 25-12.112 (Michie 1997); N.D. Cent. Code § 31-08-01.1 (1997); Or. Rev. Stat. § 40.562 (1997); Wash. Rev. Code Ann. §5.46.010 (West 1997).

The following statutes apply only to business records: Cal. Evid. Code § 1550 (Deering 1997); Idaho Code §9-417 (1997); Ind. Code Ann. § 34-42-1-2 (Michie 1998); Wis. Stat. § 889.29 (1997).

Some statutes apply to specific types of business records: Cal. Civ. Code § 2941 (Deering 1997) (notes and mortgages); Ill. Comp. Stat. Ann. 5/8-401 (West 1998) (account books and records); La. Rev. Stat. Ann. 13:3733.1 (West 1998) (financial institution records); Mich. Stat. Ann. § 21.200(131) (Law. Co-op. 1997) (documents filed under the Business Corporation Act); Miss. Code Ann. § 41-9-77 (1997) (hospital records); Mo. Rev. Stat. § 362.413 (1997) (financial institution records); Wis. Stat. § 233.12 (1997) (hospital records).

The following statutes apply only to public records: D.C. Code Ann. § 1-2903 (1998); Ind. Code Ann. § 5-15-6-3 (Michie 1998); R.I. Gen. Laws § 38-3-5.1 (1997).

Some statutes apply to specific types of public records: Cal. Gov’t Code § 68150 (Deering 1997) (court records); Fla. Stat. ch. 15.16 (1997) (records of the Department of State); La. Rev. Stat. Ann. § 13:914 (West 1998) (court records); Minn. Stat. § 15.17 (1997) (records of state agencies); N. D. Cent. Code § 54-46.1-03 (1997) (documents of the state government); Okla. Stat. tit. 11, § 22-132 (1997) (municipal records); R.I. Gen. Laws § 42-8-21 (1997) (records of the Secretary of State); W. Va. Code § 57-1-7a (1998) (records kept by state agencies or officials); Wis. Stat. § 228.03 (1997) (applies only to public records in “populous counties”).

See also, Ind. Code Ann. Court Rules, Admin. R. 13 (West 1997) (setting out optical disk imaging standards).

^{xxiii} See, e.g., La. Code. Evid. Ann. art. 1001 (West 1998); Neb. Rev. Stat. Ann. § 52.195 (Michie 1997); Okla. Stat. tit. 12, § 3001 (1997); W. Va. Code § 57-5-12 (1998).

^{xxiv} Presumably, the Regulation mandates notice to its regulators to allow them the opportunity to determine their acceptance or rejection of the chosen storage media and process. While the Regulation does not advance a particular medium, the fact that WORM optical disk does not require a waiting period once the notification has been filed indicates a potentially greater sense of inherent trust.