

Many new electronic records laws are forcing companies to rethink how they archive and protect data—or risk stiff penalties



SAVE OFTEN

By Courtney Macavinta

Tucked away in the depths of a multibillion dollar U.S. pharmaceutical research facility is a room where much of the firm's valuable intellectual property is kept. The room does not contain a refrigerator filled with vials of vaccines—it is the server room. To comply with a series of new electronic data storage laws, the company must retain all documentation relating to the development of new drugs. In fact, the growing list of data retention requirements the drug company faces is adding dozens of terabytes of data per month. As a result, developing disease vaccines or prescription medicines is no longer the company's sole mission; expertise in data storage and recovery is also a requirement for success.

On the heels of a regulatory wave in which many electronic data laws have been passed in the United States alone, more companies have to grapple with how to build IT architectures to retain data for long periods, keep data secure in its original format, and easily recover records at any time. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) state that data cannot be altered after it has been created, including medical exam records like X-rays. Whereas the Securities and Exchange Commission Rule 17a-4—combined with the Gramm-Leach-Bliley Act of 1999—requires the securities industry to maintain customer financial statements, banking records, and internal brokerage communications for three to six years, it also requires that records remain “easily” accessible for two years after they are created.

Understanding and complying with a growing matrix of state and federal laws can be a challenging task—and an expensive one. For instance, the Sarbanes-Oxley Act of 2002 was passed in response to financial scandals surrounding practices at Enron and WorldCom, and it requires publicly traded companies, accountants, attorneys, and even firms that intend to go public to retain electronic business records for five years and financial data for

seven years after an audit. To comply with Sarbanes-Oxley—which will be fully in effect by the spring of 2005—companies large and small are spending millions of dollars.

The cost of noncompliance can be high too. In addition to pharmaceutical companies, the securities, insurance, health care, financial services, consumer products, construction materials, and food transportation industries all risk litigation, fines, and criminal penalties if they do not comply with data archiving regulations. “In this arena, liability is a growing and significant issue for companies and executives,” says Shannon Kellogg, director of government and industry affairs at RSA Security, a leading cybersecurity firm based in Bedford, Massachusetts. “On the other hand, better data security can be an important enabler for companies. While decreasing legal liability, a company can increase efficiency and ensure better auditing.”

In this second part of our series on regulatory compliance, learn about why you may need to rethink your organization's storage practices

Developing best practices for data archiving

After learning which data regulations affect them, companies must ask how they can build an IT architecture that supports compliance. “The way most regulations are written, there isn't a clear road map to compliance,” says Andy Efstathiou, a technology management strategies analyst for the Yankee Group. “What eventually rises to the surface are best practices.

Companies can't ignore the regulations, but they can tailor the regulations for a mutually acceptable outcome for the government and private industry.”

Data security policy guidelines were released by the Corporate Governance Task Force in March 2004. The panel agreed that improving information security—and easing regulatory compliance—requires senior executives and board members to make information security an integral part of core business operations by adopting corporate governance controls and policies.

For industries that must comply with data privacy and retention laws, the growing response is to adopt an approach that includes processes, people, and technology to effectively manage and maintain electronic records. The key, experts say, is to balance vulnerabilities, risks, and costs with operational needs. “At its core, compliance is about protecting and managing information, as well as extracting maximum value with minimal risk,” says Peter Gerr.¹ Plans should focus on the collection, security, storage, and easy retrieval of critical data. Senior executives should consider the following aspects:

Requirements. For starters, enterprises need to determine which regulations affect them and require compliance. Many companies are getting guidance from consultants, industry associations, and external auditors.

Caring for medical records— for life

Radiology Limited is a 48-member radiology group with more than 400 employees based in Tucson, Arizona. From mammograms to MRI and CT scans, Radiology Limited handles about 600,000 exams per year. And today, the operation is almost totally digital. Gone are the days when a courier had to zip around town running film to doctors' offices. Instead, Radiology built a Dell-based architecture to transfer digital images of patient exam results to hospitals and remote radiologists for review. Referring physicians also can access images and reports online.

Digitizing radiology exams not only is more efficient, but it also can help save lives. The digital image quality is better than traditional film, and when an exam is completed, the results are available instantly instead of in one or two days.

But with the advantages of digital data comes new responsibility: Radiology must store X-rays for anywhere from seven years to the span of a person's entire lifetime, depending on HIPAA requirements and other state and federal laws.

The Radiology Picture Archiving Communications System (PACS) stores about 6 TB of data per year, and Radiology expects the amount to rise to 8 to 10 TB in the near future. The system is connected by a long-distance optical network to a duplicated storage area network (SAN) at a secondary site. This redundancy adds an extra level of data protection. "All of our storage needs are mission critical," says Eric Neid, director of information technology at Radiology Limited. "Our system currently holds all of our patient imaging data. In the near future, we would like to copy the Radiology

Information System (RIS) database to the SANs as well. Those functions, from patient scheduling to billing, are essential to our practice."

That's where Dell enters the picture. Radiology has been partnering with Dell since 1993, but to meet new data storage requirements, it needed more expertise—and equipment. First, Radiology standardized on Dell™ desktops and Dell PowerEdge™ servers.

Next, the company deployed a SAN based on the Dell/EMC CX700 storage array. The array enables hefty data transfers—and also helps Radiology meet its goal of 5- to 7-minute data backups. More important, the Dell/EMC SAN allows Radiology to meet its data storage regulations today and add storage as its data grows.

Roles. Many laws, as well as the Corporate Governance Task Force, call on senior executives to take responsibility for ensuring information security and deciding how to respond to regulations. A data security strategy should be tailored to the organization's needs, and executives should assign explicit roles, responsibilities, authority, and accountability to the individuals who should carry out the plans.

Data retention. While assessing data security needs, enterprises should determine the impact that regulations will have on their data. Where do certain kinds of data reside in the organization? What data formats do you use? How should you index files? Does data have to be maintained for long periods of time? How quickly must you be able to access it? Must it be readily accessible, even with future software? Do you need to keep data in its original format and never alter it?

Security status. Next, you should assess current data processes and security practices, including networks, facilities, and hardware. What is being stored and backed up on the network?

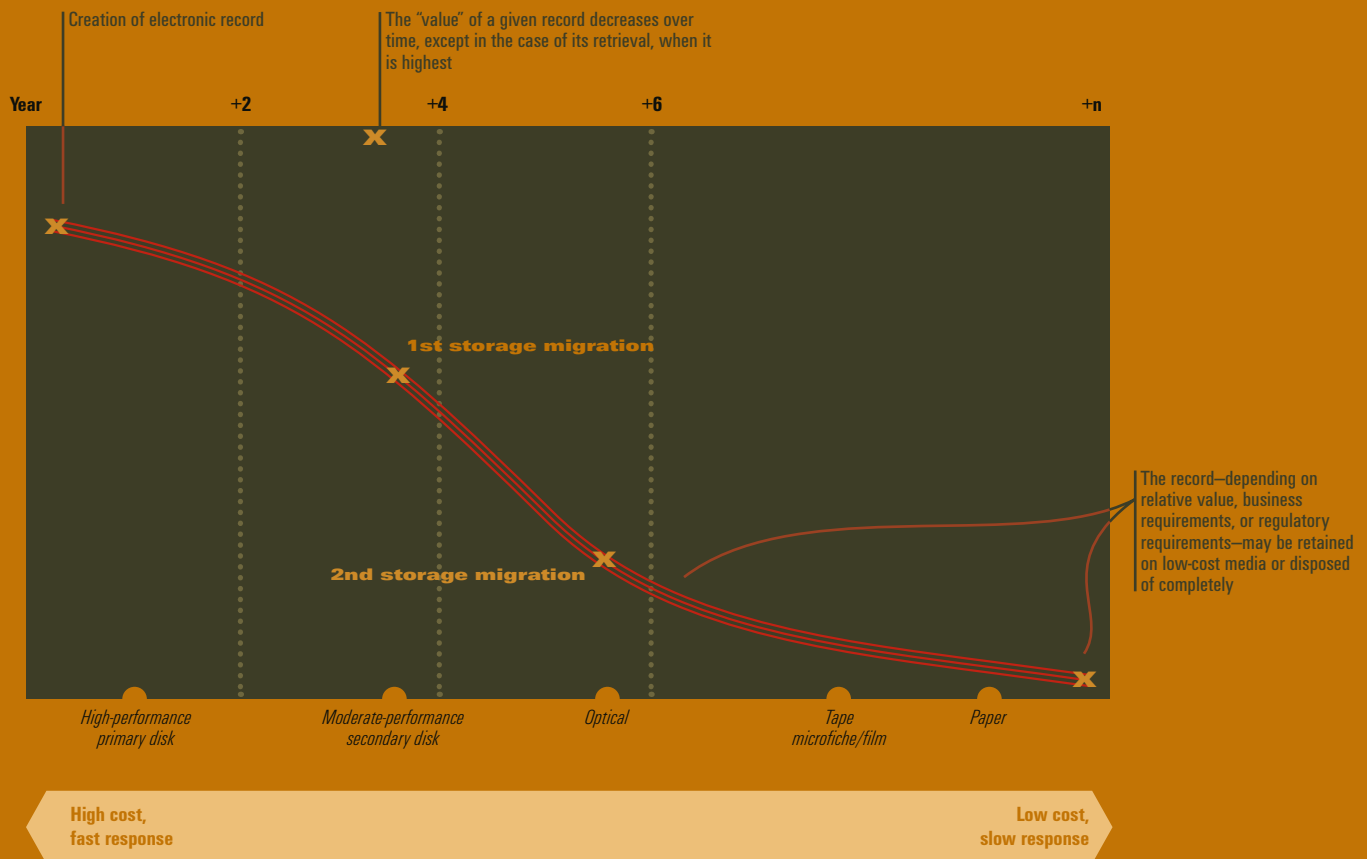
Identify security gaps and develop a plan to close them. It is essential to keep employees trained and aware as new data management and security requirements unfold. Regularly conduct periodic testing and evaluate the effectiveness of security policies and procedures, and quickly respond to vulnerabilities.

Enabling technology. Based on data retention and security requirements, enterprises will likely have to map out an architecture that automates data backup and recovery processes, includes offline and online storage, and allows for storage of media that needs to be indexed and retained for long periods of time. To comply with the Sarbanes-Oxley Act, financial services companies will have to consider whether their IT architecture meets auditing requirements. Organizations that fall under HIPAA, for instance, will have to ensure they have enough storage capacity and scalability potential as unalterable data volumes grow over time.

"To meet compliance, you have to implement solutions across multiple silos within your organization," Efstathiou says. "You

The data retention cycle

How to best manage a record depends not only on regulatory requirements, but also on how often the record needs to be accessed based on business needs and the value of a record. Here is an example of how to manage a record throughout its retention cycle:



need the ability to bridge multiple silos to create a holistic view of the organization—a view that is more cost-efficient and secure. For most organizations, it takes a fair amount of lead time to implement new solutions, test them, and work out the bugs—and most need to customize their infrastructures to a certain degree.”

Finding the right technology for the job

Based on regulatory requirements, organizations usually have to deal with two types of data: data that is unalterable and data that is alterable or removable. Unalterable data, such as permanent records and e-mail archives, usually must be kept on-site and requires a permanent storage array. Alterable or removable data can be stored off-site and only needs to be kept for a set period.

Data backups are necessary to recover lost data in an emergency, but they typically retain data for a shorter time. Data archives, on the other hand, are designed for the long term and require a combination of online and offline storage solutions. Enterprises might need to consider several IT architecture components when it comes to storing and protecting unalterable and alterable data:

Scalability. A scalable, cost-effective storage array that can grow as storage needs grow is what most enterprises need to meet the ongoing regulatory requirements.

Accessibility. A consolidated networked storage infrastructure, such as a storage area network, can help meet demands for fast retrieval and can help companies comply with laws such as Sarbanes-Oxley.

Security. WORM (write once, read many) media, which allows information to be written to a disc a single time and prevents the data from being erased, can help companies meet unalterable data storage requirements, such as those mandated by HIPAA.

Flexibility. Storage management software for archival use must be flexible to enable compliance processes based on custom-tailored company policies. Also, enterprises often need software that provides audit trails of changes made to archived data as well as reports that reflect data origin and activity.

Dell services provide reliable expertise and support

Dell provides a comprehensive set of hardware, software, and services to help meet a variety of needs for archiving important data as required by Sarbanes-Oxley, HIPAA, and many other regulations worldwide. Dell's award-winning service and support team can help you implement the right data archiving architecture for your specific environment. Dell combines its expertise with partners' capabilities to ensure that you receive the support you need throughout your data retention life cycle.

Professional services

Dell Professional Services helps optimize your return on investment by helping you design, develop, and deploy an innovative, robust, and scalable solution. Dell utilizes a proven methodology and project management expertise to understand your business objectives, design plans that are flexible to adapt to your current environment, and then deliver results.

Microsoft Office Accelerator for Sarbanes-Oxley

Dell Professional Services offers implementation of this software package, which is designed to specifically address the requirements of Sarbanes-Oxley regulations concerned with financial and accounting records. Microsoft® Office Accelerator helps facilitate compliance by addressing information management and collaboration rather than just storage. It also helps enhance reporting capabilities and can adapt to evolving requirements.

Deployment services

Dell deployment services can help you smoothly incorporate a data archiving solution into your organization. From Custom Factory Integration to custom delivery and installation, Dell helps get your data archiving system up and running quickly.

Support services

Dell offers flexible support service options that help you maximize system availability and increase IT staff productivity. Dell can provide software and hardware support along with on-site service² and several response-level options so that you can select the best plan for your requirements.

Training and certification

Dell offers business and professional technology training to help your staff make the most of your infrastructure. Dell provides training program options so you can select the instruction that meets your staff's needs. Services vary by region.

Contact Dell at dell.com/compliance to see how the right technology can help with your data archiving for regulatory compliance needs or for more information on the available services in your geographic area.



Longevity. In addition to unalterable media storage, enterprises may need a robust messaging application that allows e-mail to be accurately archived—an essential storage aspect because e-mail becomes increasingly used as “smoking gun” evidence in legal cases.

The road to compliance

No matter what data storage and security strategy an enterprise uses, IT decision makers should consider these six final questions:

1. Will content be stored and remain unaltered over the required retention time frame?
2. How will this technology stay updated to ensure long-term availability of records?
3. Does this technology enable the organization to retrieve data quickly enough to respond to a subpoena within the stipulated deadline?
4. Can this technology grow with the business and meet regulatory requirements?
5. Can this technology be used with other content-generating applications?
6. How will this data storage architecture address litigation and discovery challenges?

Revamping data storage processes does not have to be just a bureaucratic hoop-jumping exercise for enterprises. An organization's compliance-driven IT architecture can also lead to opportunity. “It's smart for you to comply with the law. In addition, this whole undertaking can be a real performance enhancer for businesses at the process level,” Efstathiou says. “By investing the appropriate amount of time architecting and thinking strategically, you can satisfy regulatory requirements while you develop a better understanding of your own business.” **D**

¹ Enterprise Strategy Group. “What's in Store for 2004—Compliance, Storage, and Beyond” by Peter Gerr. February 2004.

² Service may be provided by a third party. Technician will be dispatched if necessary following phone-based troubleshooting. Subject to parts availability, geographical restrictions, and terms of service contract. Service timing dependent upon time of day call placed to Dell. U.S. only.