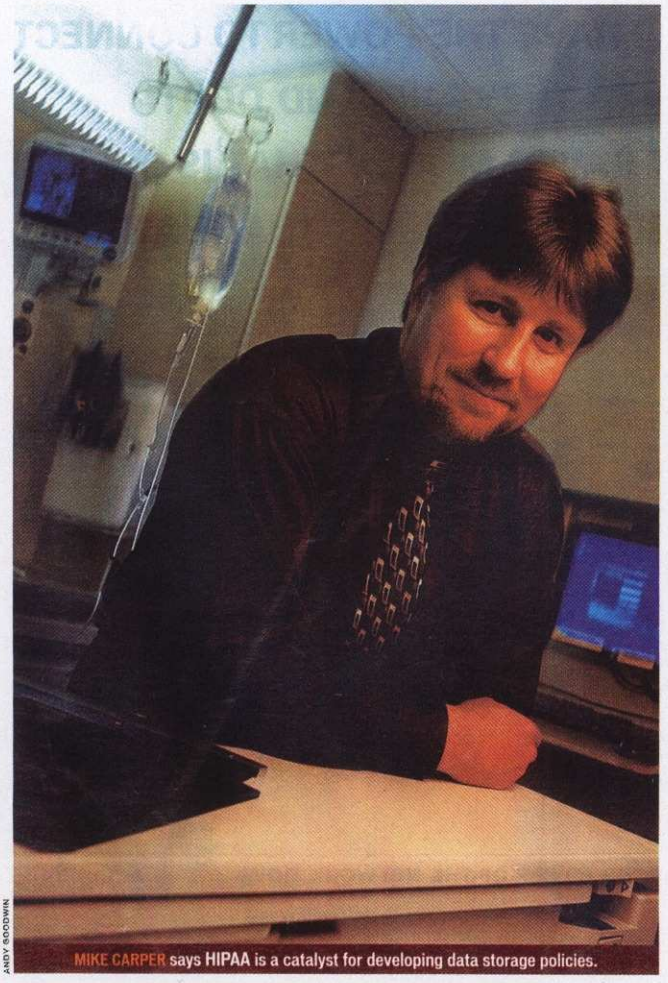
COMPUTERWORLD
THE VOICE OF IT MANAGEMENT • WWW.COMPUTERWORLD.COM
NOVEMBER 17, 2003 • VOL. 37 • NO. 46 • $5/COPY

Regulated Storage



ANDY GOODWIN

MIKE CARPER says HIPAA is a catalyst for developing data storage policies.

New rules are forcing companies to buy more storage and develop new policies around its use. By Robert L. Scheier

DRIVEN BY CORPORATE scandals and privacy concerns, new laws and regulations are requiring organizations to store more data, keep it longer and make sure it's accurate and easy to retrieve.

In response, customers are buying more storage capacity and developing new storage policies to ensure that they comply with regulations such as the Health Insurance Portability and Accountability Act and the Sarbanes-Oxley Act.

Here's a look at these two storage-intensive regulations and how some organizations are keeping to the letter of the law while getting business benefits from their compliance dollars.

Health Insurance Portability and Accountability Act (HIPAA)

WHAT IT ENTAILS: Encourages the use of electronic transactions to increase efficiencies in the health care field. Security rules require health care providers and insurers to protect patient information and to ensure its availability in case of disasters. Requires medical records to be kept in their original form for two years after the patient's death.

INDUSTRIES AFFECTED: Health care providers, health care insurers and health claims clearinghouses.

ENACTED: August 1996

COMPLIANCE DEADLINE: April 21, 2005, for most covered entities; small health plans have until April 2006.

REGULATION ROAD MAP: Experts advise IT departments to consider new optical technologies for long-term storage of records and say productivity and customer-service improvements could help pay for HIPAA compliance.

Peter Gerr, an analyst at Enterprise Storage Group Inc. in Milford, Mass., says HIPAA's requirements for long-term storage of medical records will force health care providers not only to buy more storage, but also to create policies to manage it. A typical hospital generates 50TB to 70TB of magnetic resonance imaging and computerized tomography data per year and, in some cases, will need to keep and be able to access that data for decades.

USER APPROACH: For Northwestern Memorial Hospital in Chicago, one of the first steps toward meeting HIPAA

Continued on page 36

Continued from page 32

regulations protecting patient information was to buy a 12TB EMC Corp. Symmetrix server.

Buying the storage-area network (SAN) to store and manage "things as mundane as e-mail or user files" was only the beginning, says Mike Carper, Northwestern Memorial's director of technology management. The hospital used HIPAA as the springboard to upgrade its network, its access control software and even its 5,700 client PCs to a common version of Windows XP. Users can now save data onto the SAN, not their local hard drives.

"We're using HIPAA as a tool to help develop policies around data storage," which was a task the hospital had to confront, with or without the regulations, says Carper.

Northwestern Memorial is also using HIPAA as an opportunity to upgrade its overall security capabilities. It's using Novell Inc.'s NetWare to provide role-based access-control and audit capabilities, along with the ability to audit which users have accessed which files. Carper says the hospital is also using Novell's ZENworks management software to provide role-based application access, so when data entry clerks log on, for example, they see different sets of applications than physicians see.

Brooklyn's Maimonides Medical Center migrated to two geographically separated SANs about two and a half years ago, says Mark Moroses, senior director of technical services.

Complying with HIPAA wasn't his aim at the time, he says. Moroses' goal was to handle the growth in data in his electronic medical record application and meet existing state and federal requirements to store patient records for at least seven years.

Meeting HIPAA's requirement for audit trails was a "pretty straightforward" process of "keeping more log files for a longer period of time," says Moroses. The disaster recovery requirements of HIPAA were met by using the second SAN with a replicated version of the patient data. Using an IBM FASt Storage Server managed by DataCore Software Corp.'s SANSymphony allows him to mix and match drives from different vendors as the price of storage falls and the medical center's needs grow.

As part of its HIPAA compliance, the Office of Group Benefits in the Louisiana Department of Natural Resources bought a 5TB IBM Enterprise Storage Server to consolidate data that had been stored on approximately 20 servers, says CIO Rizwan Ahmed. The SAN, along with policy-based access-control software and fingerprint scanners to authenticate users, cost about $750,000.

> **[Buying a SAN to store and manage] things as mundane as e-mail or user files [was only the beginning.] We're using HIPAA as a tool to help develop policies around data storage.**
>
> **MIKE CARPER**, DIRECTOR OF TECHNOLOGY MANAGEMENT, NORTHWESTERN MEMORIAL HOSPITAL

Yet Ahmed says, "We've saved at least as much as we spent" in increased productivity and improved customer service. He says he hopes to eventually use the centralized database to provide instant claims payments to doctors, which would cut administrative costs and "allow us to attract more and more providers, and the more providers we have, the more members we can attract."

Sarbanes-Oxley Act

WHAT IT ENTAILS: Tightens corporate reporting and audit practices; requires the retention of all working papers, correspondence and communications about a public company's financial statements for seven years.

INDUSTRIES AFFECTED: Accounting firms that audit the financial statements of publicly traded companies, although the companies themselves may also wish to retain the records.

ENACTED: August 1, 2002

COMPLIANCE DEADLINE: Most public companies must comply by June 15, 2004; smaller U.S. business and foreign companies must comply by April 15, 2005.

REGULATION ROAD MAP: Experts suggest that IT departments work with their business managers to proactively develop policies and storage architectures that aid compliance. They should consider new optical and disk-based storage technologies as a complement to tape for archival storage.

Gerr recommends that business and IT managers work together to "understand the requirements that affect you, identify the data and content types that are required to be retained and for how long, and develop auditable processes" to ensure that data is protected.

New technologies such as ultra-dense optical and relatively low-cost, high-performance Serial ATA-based disk drives can be used to create multiple tiers of storage, says Gerr. These technologies, along with policy-based storage management tools, allow customers to "tier applications and storage infrastructure by type, value, performance, availability needs or other meaningful criteria," he says.

"Fibre Channel or SCSI [storage] might be Tier 1," says Gerr. "Serial ATA-based storage could be Tier 2; tape might be Tier 3." Each successive tier will consist of less-expensive, but slower, storage that allows companies to move data to different storage levels as their importance changes over time.

To comply with Sarbanes-Oxley and other regulations, Gerr says, a company might need to be able to retrieve financial statements very quickly in the first 30 days after the end of the quarter and thus keep that data on the first tier.

"After the first 30 days, you may need to keep them online until the quarter ends, but since you don't need to access them regularly, you may want to move them" to Tier 2 storage, says Gerr. After the end of the quarter, when the need for quick retrieval of the data becomes even less likely, the company might want to move those records to lower-cost but slower-performing tape in Tier 3.

Gartner Inc. analysts Debra Logan and Rich Mogull argue that the first priority for storage or IT managers should be understanding which applications and which technologies are most critical to the law's goal of "improving transparency and accountability in business processes and corporate accounting."

"The only technology category that the law mentions specifically is 'electronic communications,' but we know that financial accounting systems, enterprise resource planning, general ledger and supply chain management systems will all be subject to the regulation," wrote Logan and Mogull in an October report. Since Sarbanes-Oxley is primarily concerned with corporate financial processes, they say, "CIOs should pay the closest attention to ERP and other financial management systems."

USER APPROACH: Tektronix Inc., a Beaverton, Ore.-based manufacturer of test, measuring and monitoring equipment, won't need new hardware or software to comply with Sarbanes-Oxley, says IS director Callie Gates. The company already purchased a SAN as well as automated off-site tape backup and archiving software from OuterBay Technologies Inc. in Campbell, Calif., as part of an information life-cycle management plan begun in 1999.

The strategy was spurred by a series of divestitures that forced Tektronix to reorganize how it handles information. While the changes Tektronix has already made put it in good shape to comply with Sarbanes-Oxley, Gates says the law will force her company and others to formalize their procedures for safeguarding data.

"Everyone has controls around this process, and the auditors document them at a high level," she says. But producing a detailed list of those processes "has never been a requirement for corporate America before," says Gates.

Gartner research conducted before Sarbanes-Oxley was enacted showed that while companies may have had adequate controls over paper records, their control of electronic documents was inadequate.

Although good record-keeping processes aren't specifically mentioned in these acts, "the implications for records management are clear."

42401

Scheier is a Computerworld *contributing writer in Boylston, Mass. He can be reached at rscheier@charter.net.*

TEST YOUR KNOWLEDGE

There's been a lot of talk about the effect of new federal regulations on corporate storage policies. Take our online quiz to see if you can separate the facts from the hype:

QuickLink a3780
www.computerworld.com