

Backups Essential

s wildfires raged last October through Southern California, staff at Skilled Healthcare watched the inferno from their Foothill Ranch office.

The building houses no residents; it is a hub for administrative services, including information technology (IT), provided to 74 nursing facilities, 12 assisted living communities, and a rehabilitation and hospice company that are part of the Skilled Healthcare Group.

At first, only a plume of smoke was visible from the building's back yard, says Allan Crommett, senior vice president and chief information officer. By the second day, the plume was larger as the blaze—which had been set by an arsonist and was one of many fanning throughout the region—grew.

The next day, the flames were still a couple of miles away but began “jumping over” the toll road that runs past the building, Crommett says. By the fourth day, the road had been closed, the blaze had arrived across the street, and “the whole valley had filled with smoke,” he recalls. Staff were sent home, taking laptops that would allow them to continue doing at least some parts of their jobs.

Being Prepared

Despite the proximity of the fire, it remained under the control of firefighters and never posed a serious threat, Crommett says. If it had damaged the center, however, the company would have lost none of its essential clinical or financial information and would have had uninterrupted access to the files, since all of

the information is stored at a data center in Milwaukee. Information on residents' current treatment and medication orders are maintained there, integrated with the minimum data set (MDS), admission, and billing records.

All Skilled Healthcare facilities are “tied in directly to the data center,” which hosts the applications, Crommett says. “None of those [facilities] have their own applications or databases on site.” In the event that the data center itself were threatened, it, too, has a distant secondary backup site from which information could be retrieved.

“On the IT side, our goal is to focus on business continuity,” allowing facilities to focus on keeping residents safe and providing care during disasters or other emergencies, Crommett says. The system was tested when Hurricane Rita swept the Gulf coast and one of Skilled Healthcare Group's facilities in Beaumont, Texas, had to evacuate residents to other facilities within the network.

“Merely by updating security for nursing staff at those [receiving] locations, we could allow them to get to [resident] records,” Crommett says.

The company is piloting an expansion of its electronic record system with a wireless bedside charting system used by certified nurse assistants (CNAs). Ultimately, this information will become part of the integrated electronic record, retrievable from the data center.

Continuity Of Care At Stake

Like most long term care organizations that are making the transition to electronic health

Having EHRs in place is not enough: Providers need

For Resident Records

Lynn

FPO

to have off-site duplicates in case disaster strikes.



Chris Canagarajah/sanjour.com

Skilled Healthcare staff watch from their Foothill Ranch, Calif., office as wildfires race through the hills.

records (EHRs), Skilled Healthcare is taking an incremental approach, and, with every new advance, the organization's electronic records system gains in comprehensiveness and immediacy.

Few, if any, of these initiatives are driven primarily by the need to shore up disaster recovery capabilities. In a post-Katrina era, however, the critical nexus between health information technology (HIT) and disaster planning is increasingly recognized by providers and technology advocates.

The medical record "is a lifeline for the business," says Michelle Dougherty, director of practice leadership at the American Health Information Management Association in Chicago. In the midst of a disaster, continuity of care for dislocated residents depends on the availability of information about their current treatment and medication needs, Dougherty says.

When paper records are destroyed, the information is lost and cannot be recaptured, but, with electronic records, providers gain "the ability to archive data and retain it in places that can be accessed remotely or from other locations when they need it," Dougherty says.

The value of electronic medical records is one of the "hard-taught" lessons of Hurricane Katrina, which left a trail of ruined paper records in flooded offices, says Roxane Townsend, assistant vice president of health systems at Louisiana State University (LSU) System in Baton Rouge.

The legendary storm also demonstrated that EHR adoption alone is not enough—it must be coupled with a disaster recovery plan that provides for the protection and accessibility of electronic records, Townsend says. Some clinics and physician practices in the path of Katrina, for example, had implemented EHRs, "but the servers were in the office and under water," revealing the vulnerability of electronic records that have not been backed up in a location that is out of harm's way, Townsend says.

Summing up this second hard-won lesson, she warns, "Don't put your redundancy in the same area that's hurricane- or flood-prone—and don't put it on the bottom floor."

Planning In The Electronic Age

As providers adopt electronic records, they must "reinvent their disaster plan" to ensure that records are protected

and fully leveraged for the advantages they offer in a disaster scenario, says Maria Moen, president and chief executive officer of Carrollton, Texas-based HealthWare Consulting Services, which specializes in HIT installations in long term care settings.

This should include a process for backing up electronic medical records to ensure that data aren't lost or compromised in a disaster and a plan for recovering data in a reasonable period of time, experts say.

Electronic medical records give providers "a big jump on the preservation of information," says Dan Cobb, chief technology officer and co-founder of HealthMEDX, a long term care software firm in Ozark, Mo. To realize that value, however, the "best practice" is to back up the data and store it off-site, so that electronic records are not destroyed if the facility is impacted by a disaster. Providers also need contingency plans for accessing information in a disaster, Cobb says.

Key Objectives

Disaster planning for IT should be built around identified risks to the facility and its data, so that providers can anticipate and plan for relevant events, says Jonathan Thompson, vice president of Healthia Consulting in Golden Valley, Minn. The plan must also prioritize data needs to determine what information is most critical to the organization and would have to be recovered first in a disaster.

Providers also need to determine what they can afford, as safeguards such as off-site backup, redundancy, and data retrieval are costly, Thompson says.

Healthia, which has managed several disaster recovery projects, has identified three core objectives for the IT disaster plan:

■ *High availability.* This is the preventive component of the plan. An organization's IT infrastructure should be designed to ensure that it will be operational and keep data available to

users 99.999 percent of the time, Thompson and other IT experts advise.

Commonly referred to as the “five nines,” this is the threshold deemed appropriate by IT experts for access to critical data and applications. A lesser standard of 99 percent might seem reasonable, but with 8,760 hours in a year, 1 percent down time would translate to 88 hours, or 3.6 days, over the course of a year in which data was not available, Thompson says. For many health care providers, that is not acceptable. “It could be an issue with patient care,” he says. “What do you do with the time when electronic data is not available?”

Meeting this standard requires “redundancy in the network,” which in turn requires additional computers, servers, even a “hot site,” a secondary location—preferably outside the area that would be affected by the same disaster—where data from the primary site is mirrored, Thompson says.

■ *Disaster recovery planning.* The recovery plan is triggered when the high-availability process fails, and providers experience down time, during which they lose access to electronic records, Thompson says. The disaster recovery plan should define the process for regaining access to data. “Literally, it is a list of who does what and the steps to recovery,” Thompson says. The plan should include workflow and checklists, he adds. “It should be actionable and understandable.”

■ *Business continuity planning.* This defines how the business will operate in concert with the IT disaster plan to maintain critical operations during the down time, Thompson says. For example, if an EHR is not available, the business continuity plan should describe how patient information will be accessed.

The Compatibility Issue

Moen says disaster plans should take into account the possibility that residents will have to be evacuated to

Captial Source

Business Continuity Checklist: Preparing For The Worst



An annual AT&T survey measuring the readiness of U.S. business for disasters found that 26 percent of the 1,000 information technology (IT) executives interviewed did not consider business continuity planning a high priority and had no plan in place for sustaining critical operations in the event of a disaster.

Respondents to the 2007 survey represented companies with revenues of more than \$10 million in 10 cities around the country.

While health and long term care providers tend to lag behind other types of businesses in technology adoption, the AT&T survey revealed a more generalized lack of preparedness in the private sector when it comes to protecting data and technology from the impact of disasters. Business continuity planning helps organizations ensure that they “can recover the technology and processes required to operate after an unforeseen failure in normal operations,” AT&T says.

Results from the 2007 survey, however, “suggest that companies may have a false sense of security,” said Jerry Shammas, AT&T’s executive director of business continuity and recover services, in an interview on the company’s Web site.

“More than 50 percent believe the

system they have in place is sufficient,” he said.

Specifically, 52 percent of respondents said they had no plans to improve business continuity planning in the next six months, while only 16 percent said they planned to establish redundant servers or backup sites for data.

AT&T, which markets business continuity planning as one of its services, offers a business continuity checklist on its Web site that includes the following actions:

Planning for the impact of an unexpected or catastrophic event on your business:

- Identify a coordinator and/or team with defined roles for preparedness and response planning.

- Conduct a business process and services inventory to understand which processes are mission-critical to the survivability of the business.

- Determine acceptable levels of service during the recovery period and what processes need to be maintained or restored first to keep the business running.

- Identify the essential employees and other critical inputs (sub-contractors, services, logistics) required to maintain business operations by location and function during the event.

- Conduct a technology asset inventory to determine and document the mission-critical technology components, their locations, how they’re configured, and who is responsible for their management.

- Once key components are identified, determine what measures should be taken to protect and recover them.

- Understand the rules or regulations governing your business operations. If you had a business failure, would you be able to maintain compliance?

- Identify a budget.

Assessing data and technology needs in the event of a failure in operations:

- Determine the status of your existing disaster recovery plan. Do you have one, and is it maintained? Have you tested the plan?

- Determine vulnerability of your organization’s technology infrastructure to natural disasters, including floods, fires, earthquakes.

- Set clear recovery time objectives for each of your business/technology areas.

- Determine the need for off-site data storage and backup.

- Develop a technology plan that includes hardware, software, facilities, and service vendors.

Source: AT&T

locations that do not have compatible medical record software. As a result, it may not be possible to access data from a receiving facility’s computer.

To address this possibility, one of Moen’s paperless clients has worked with its software vendor to develop a program that retrieves a high-priority subset of resident data at designated

intervals throughout the day from the facility’s computer system and downloads it to several portable drives. The data include current physician, medication, and treatment orders; recent nursing notes; demographic information; advance directives; and basic financial information, Moen says.

The facility maintains multiple

drives, which could be picked up and transported to another location in a disaster. The backup program converts the data to a common, readable PDF format.

“The key to this data dump was to make sure that it output data to a portable drive that [designated staff] could pick up and take with them in a

disaster” so that it could be read in a common format at the receiving location, Moen says.

Safeguarding Electronic Records

There is no fixed model for this new breed of contingency plans for electronic medical records, and providers are employing a variety of strategies tailored to their individual risks, organizational structure, electronic capabilities, and resources.

Golden Living, in Fort Smith, Ark., provides centralized backup for the electronic clinical records generated by 334 independently operated skilled nursing facilities and 18 assisted living communities around the country.

Electronic records contain care plans, medication and treatment orders, the most recent care activities, and nursing notes, says Chuck Goux, vice president of information technology. Data are backed up frequently, ensuring that new information is captured almost as soon as it is entered, he says. The centralized database is further backed up by data centers in Kansas City and Denver.

Goux started with the company 11 years ago, when it was Beverly Enterprises. At the time, the average facility “had one or two PCs and no connectivity,” he says. “We used a lot of Excel spreadsheets and were very manual driven.” When a facility was impacted by flooding, or when extinguishers or sprinklers were used in a fire, “records got wet.”

Now, data losses only impact information that is being entered or transmitted at the moment a computer goes down, Goux says.

Last year, when a couple of facilities were affected by flooding, staff didn’t worry about gathering records. Instead, they spent their time preparing residents for evacuation, making sure they had oxygen and other essential equipment, says Goux. The facilities’ IT systems were shut down, and staff were able, from alternate locations, to seamlessly access residents’

Consumers Support Electronic Records

Consumers significantly overestimate the use of electronic medical records by their physicians, according to the results of focus group interviews and a telephone survey conducted last June for the Washington, D.C.-based eHealth Initiative Foundation.

Forty-five percent of respondents said they believed their physician kept their medical records in electronic form, and 64 percent believed that an electronic backup copy was kept off-site. The latest data from the National Ambulatory Medical Care Survey indicates that, in fact, only one-quarter of office-based physicians use partial or full electronic medical record systems.

The research, conducted in the five Gulf states of Alabama, Florida, Louisiana, Mississippi, and Texas, found that respondents placed a surprisingly low priority on the exchange and transmission of electronic medical records “during or after natural disasters.”

Though respondents came from a region hard hit by hurricanes in

recent years, only 9 percent identified natural disasters as the top reason why they would want access to a health information exchange (HIE), making it possible for their

medical records to be shared and accessed electronically.

The vast majority (70 percent) supported the development of HIE.

Forty-six percent said the most important reason to have access to such a network was for emergency medical situations, followed by access to medical records when traveling out of state (14 percent), having access to medical history for physician visits (10 percent), having access to medical records during or after natural disaster (9 percent), transferring laboratory and X-ray results between providers and having access to a medical history when refilling prescriptions (5 percent).

Public Opinion Strategies, which conducted the research, based its findings on a combination of 1,000 telephone surveys and 1,000 focus group interviews with consumers, physicians, and employers.

records from the backup database, using a secure Internet connection.

Golden Living is moving in stages toward a full-blown EHR, Goux says. By April, all facilities will have wireless capability, enabling the use of handheld and other wireless devices.

Also in April, the company will launch a pilot of electronic medication management, with a roll-out planned to all facilities by late 2009, Goux says. The system will capture information in real time, “the instant medication is administered,” Goux says. “It will be a tremendous advantage to have that capability.”

Golden Living is also planning to

pilot a bar-coded bracelet, which could be used during disasters to quickly identify relocated residents and call up their immediate medical needs. When the bracelet is scanned, it will show, for example, that a resident with diabetes has been traveling for several hours and is due for insulin, Goux says.

Currently, the organization’s electronic record consists of an MDS-based clinical application, which has been upgraded to give it some aspects of EHR functionality, Goux says. It is integrated with an application, called Care Tracker, which CNAs use to document their care and assistance with activities of daily living (ADLs). From

IT Disruptions: Another Type Of Disaster

Disaster plans should also envision the management of IT disruptions created by human error, says Jonathan Thompson, vice president of Healthia Consulting in Golden Valley, Minn.. Missteps that occur during the implementation of a system change, for example, can “bring a production application to its knees and cut off access,” he says.

“Is this a disaster? Not in the traditional sense,” Thompson says.

“But when it prevents access to a host of end users, the term disaster needs to be redefined” to include those situations, he says.

Changes made to the system in response to user demands account for a growing share of IT disasters. “I see more and more that that is the cause of down time,” he says.

Unintentional human error accounts for 50 percent to 80 percent of IT disasters, Healthia reports, citing data from Computer Security Management. Only 10 percent to 15 percent of failures are the combined result of natural disasters—including floods, earthquakes, hurricanes, and tornadoes—and man-made disasters, such as loss of power, chemical spills, or transportation accidents.

Dishonest employees account for 10 to 17 percent of IT disruptions, while employee sabotage, water

damage, and acts committed by persons outside the company account for much smaller percentages of IT crises, Healthia reports.

Managing Change

Problems stemming from system changes have become so commonplace that Healthia has developed a best practice for the “change management” process, Thompson says.

Healthia’s best practice for change management starts with defining who has the ability to decide that the change should be made and identifying the stakeholders in this particular system change, the potential impact of the change, and a “work-around” to avoid negative impacts on other applications, Thompson says.

“Part of the solution may be to educate the end user that it is not possible to make that change because there are too many other impacts,” Thompson says.

Applying this best practice “means having 20 to 30 people reviewing the list of proposed changes, identifying their potential impact,” and bringing “all hands on deck” when the change is implemented to make sure there are no glitches, Thompson says. Because this is an onerous process, “a lot of organizations don’t do it,” he adds. But it can help to avoid disastrous consequences.

centers that it owns and maintains within a 50-mile radius. The centers are close enough to give the Sioux Falls IT staff access to them, but far enough away to be outside of the tornado pattern, which poses the greatest weather risk to the Sioux Falls area.

As recently as three years ago, this arrangement was unique, but today many organizations are taking a similar approach, says Rusty Williams, chief information officer and vice president of information services and technology.

The two data centers, called “hot sites” for their readiness to provide immediate recovery functions, operate from different power grids and use different Internet service providers. This ensures they would not both be impacted by a single power or connectivity failure. The centers are networked together, however, so that the data are mirrored in both places, and each runs duplicate clinical, billing, and other key applications. Good Samaritan’s 240 facilities, which access the network through a Web browser, can take either path.

As a result, from a user standpoint, disruptions to the system, no matter what the cause, are fleeting.

“If an application fails in one place, it is up and operational for the rest of the organization in a quick time frame,” says Williams.

Good Samaritan also uses its redundancy for planned outages that occur with upgrades or system servicing. System upgrades can take half a day and cut users off from critical applications for an extended period. This is not only inconvenient, but costly, says Williams, citing the example of the time and attendance application, which records information for 23,000 employees.

“If that’s down for a single shift, think of all the manual work that has to be done just for payroll,” Williams says.

“Part of the key to making this work for us is to have a fully functioning network running at both data centers,

a computer kiosk stationed in each wing, CNAs swipe their identification badge to call up the list of their residents, along with symbols representing care activities and assistance with ADLs, such as showering, dressing, and meal intakes. As CNAs select the appropriate symbols, information populates the medical record to reflect the care being provided. The program has

improved the accuracy and consistency of documentation, and “CNAs love it,” Goux says.

A Double-Up Backup

The Evangelical Lutheran Good Samaritan Society in Sioux Falls, S.D., has also built in significant redundancy to its centralized electronic record system, with two dedicated backup data

which eliminates a network recovery effort” in the event of a disaster or outage, says Jim Consoer, director of data center operations.

IT Recovery: A Complex Process

The disaster recovery process for IT is complex, requiring careful planning and an impact analysis to establish priorities for data retrieval and recovery times for individual applications.

“Each application has its own priority,” Consoer says. The recovery time for some is five minutes, while for others it is 24 hours or a week. “Not all processes are equal,” he adds. “A health care record would certainly have a higher business impact than recovery of a spreadsheet,” so the recovery plan would target medical records first.

Recovery is never 100 percent, Williams says. The goal is not to retrieve every document, but “to mitigate the impact [of the event] on the business,” Williams says.

Currently, Good Samaritan’s electronic records are comprised of a mix of applications that are both vendor-purchased and self-developed, Williams says. The primary modules contain care plans; physician, treatment, and medication orders; and the MDS.

This year, Good Samaritan plans to take significant steps toward becoming less dependent on paper. Though no timeline has been set for implementation, the organization is in the process of selecting a vendor for a comprehensive EHR.

As an interim step, a wireless documentation system, called “Hands On,” will be implemented early this summer, Williams says. The system will enable clinical staff to use hand-held devices to record assessments in real time. The eight modules that comprise Hands On are ADLs, bathing, toileting, care plan approaches, dining, mood and behavior, skin, and vital signs/weights/heights.

As Good Samaritan’s IT infrastructure evolves, disaster recovery becomes

Disaster Recovery Plan Development



- Deploy “quick-hit” solutions
- Develop high-level recovery strategies and recovery phases
- Define roles and responsibilities, including line of command
- Define disaster assessment and declaration definitions and procedures
- Develop emergency/evacuation procedures that incorporate disaster recovery plan activities
- Document organization, staff, and system functions and recovery requirements and procedures
- Establish recovery locations and document steps to make functional during a disaster
- Develop business partner and vendor agreements
- Develop communications plan and identify alternative communication tools
- Create contingency plans for missing people, failed procedures
- Build maintenance schedule and procedures

Source: Healtbia Consulting: “Creating an Actionable Disaster Recovery Plan”

more complex. The growing number and increasing complexity of applications means more intensive recovery work to maintain critical operations, Williams says. The burden is far outweighed, however, by the “tremendous advantage of having those documents electronically.”

Katrina Looms As Cautionary Tale

For some victims of Hurricane Katrina, the difference between having

an electronic health record and not having one was a matter of life and death, says David Merritt, project director for the Center for Health Transformation (CHT) in Washington, D.C.

A vivid example involves a clinical trial sponsored by the National Cancer Institute (NCI), Merritt says. Many patients from the Gulf region were participating in the trial, and when they fled the storm their care was picked up at area hospitals.

“Their [medical] information was available instantaneously” because it was in electronic format in the NCI network, Merritt says.

Hundreds of other cancer patients who had also been receiving chemotherapy but were not part of the NCI trial also ended up at local hospitals, says Merritt. These patients had “no information on which to base treatment,” Merritt says. All physicians had to work with was what patients could tell them.

It is not possible to assess the exact cost—in dollars and lives—of recreating the treatment regimen for these patients, Merritt says. Anecdotal reports, however, suggest that it cost millions, and many died, he adds.

“Cancer killed them, but lack of information did also,” Merritt says.

National Progress Slow

The widespread loss of health records from Katrina was expected to ramp up EHR adoption and development of the infrastructure needed for a national health information exchange network.

According to Merritt, however, none of that materialized. “I can’t point to a single thing in the sphere of health information technology that was inspired by Katrina,” he says. “There has been a lot of talk, not a lot of action.”

In spite of the federal level activity that has swirled around HIT, particularly the creation of standards, Merritt says the efforts pale in comparison to what is needed.

CHT has been an advocate of a massive federal plan to fund the development of an electronic superhighway, on a scale comparable to the Eisenhower administration's investment in the interstate highway system. Signed into law in 1956, the Federal-Aid Highway Act called for more than 40,000 miles of interstate highways, at a cost of \$25 billion—at a time when the entire federal budget was \$70 billion, Merritt says. That 10-year project was initially undertaken for national defense reasons, as part of the country's "disaster preparedness and ability to respond to a nuclear attack from the Soviet Union," Merritt says.

While it was never used for that purpose, it has been used on occasion for mass evacuations, such as when Hurricane Rita hit the Gulf Coast.

Like the interstate system, an electronic superhighway would be essential to the management of a national or regional emergency, but it would also have tremendous peacetime value, used "by every doctor and provider in the country," Merritt says. "If the federal government is serious about building a modernized HIT network, it should put a project on a scale with that."

Louisiana Moves Forward

The state of Louisiana, meanwhile, has invested significantly in creating an electronic network, spending \$54 million in last year's budget alone, says LSU's Townsend.

In the wake of Katrina, a coalition of eight providers and payers formed to develop a health information exchange (HIE), Townsend says. Organizations that were competitive in the marketplace set aside their proprietary interests to advance the prospect for electronic records.

Two years ago, the group created the "conceptual architecture" for HIE, Townsend says. While it didn't work as planned, there are now "off-the-shelf products that will do what we couldn't get this system to do," she says. "We still think it is extremely important.

The ultimate goal is for everyone in Louisiana to have [an EHR]."

The state has invested \$30 million in the LSU system for the implementation of a fully functioning EHR, she says. As a result, all 10 of the hospitals in that system will make "significant progress this year," Townsend says.

In addition, a group of seven rural hospitals in northern Louisiana received a total of \$13 million to fund the adoption of EHRs and the infrastructure to exchange data.

"What we're most excited about," she says, "is that the state put \$10 million into Medicaid for health information exchange on a statewide basis."

Together with the Ochsner Health System, which has an electronic record system in place, these initiatives lay the groundwork for a common architecture that can be adopted on a statewide basis and connect these various efforts,

Townsend says. "Are we where we would like to be?" she says.

"Absolutely not."

By 2010, however, she predicts that Louisiana will be well on its way to statewide EHR adoption and networking. By 2014, "we'll have a majority of providers" working with interoperable EHRs, she says. "The first hurdle is to get practitioners to start collecting information in an electronic format so they can exchange it."

It has been easier to move Louisiana providers, Townsend says, because of their experience with Katrina. "If you have one major disaster, it levels the playing field and makes everyone realize how important it would have been to them" to have had electronic records, she says. ■

LYNN WAGNER is a freelance writer based in Shepherdstown, W.Va.