Abstract: From angry employees to acts of God, threats to an organization's data security abound. The key to averting disaster or minimizing its effects is a solid data security plan. This article describes the many types of data risks that exist, offers suggestions on how to develop a plan to counteract them and defines nursing's role in ensuring the safety of health and patient data.

Preparing for the Unthinkable: What to do Before Disaster Strikes

In the hours after the tragic collapse of the World Trade Center, one of the images we saw over and over again was the snowstorm of paper that came down on city streets and neighborhoods as far away as Brooklyn – paper records of financial transactions, once-confidential files, proprietary information and internal memos – all scattered to the wind in an informational blizzard. These days, most records are backed up electronically. However, in the case of a far-flung disaster like the World Trade towers, the businesses housed there also lost all of their computers and whatever backup files were stored on the premises.

Thankfully, most healthcare organizations will never experience a disaster of even one-hundredth the magnitude of what happened in New York City last September. Yet more so than any other industry, healthcare must be prepared. Unlike other businesses that may simply shut down during a catastrophic event, hospitals, nursing homes and other care facilities must remain open and operational. In fact, they may even be called upon to provide trauma and emergency care to disaster victims, requiring them to function at full capacity. And of course, data is crucial to healthcare operations: Information from the lab must get to physicians, patient information such as allergies and pre-existing conditions can prove critical, interventions must be documented and made accessible to the entire care team. The catch is, the only way all this can happen is through preparedness. As managers and administrators, it is our duty to be familiar with our organization's disaster plan and the responsibilities that will fall to us should the unthinkable happen.

Defining disasters

From an informational technology (IT) standpoint, a disaster can be defined as an event that creates an inability to maintain the flow of data necessary for critical operations, over a prolonged period of time. This might mean that data has been lost and is completely unavailable, or that data is temporarily irretrievable (it can neither be accessed nor updated). The events that can lead to such disasters can be lumped into three broad categories.

1. *Natural disasters:* Fires, floods, earthquakes, tornadoes, hurricanes, ice storms and most other weather-related incidents; the proverbial "acts of God."
2. *Manmade disasters:* Labor strikes, vandalism, theft, computer crimes and acts of terrorism.
3. *Technical disasters:* Power outages, application failures, phone line outages, operating system failures, hardware failures, loss of stored data and Y2K.

Unpredictability is a hallmark of disaster. Even if you know what types of disasters are possible, there's seldom any way to anticipate which type will befall you. The key therefore is to be prepared for all types. Fortunately, there are a few folks who make it their job to see to it that you are.

Legal and accreditation requirements

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), along with its mandates for patient privacy, also requires that every healthcare organization (including insurers) have a disaster recovery plan (DRP) in place. The plan must be tested to ensure that it can facilitate restoration of systems, network and data following a catastrophe. The plan must provide for both *immediate* and *temporary* recovery from the event. However, if normal conditions aren't restored within a short time, a longer-term strategy, the emergency-mode operating plan (EMOP), kicks in. This plan, which is separate from the DRP and takes over where it leaves off, must ensure operational continuity for some time following the catastrophic event.

Data security has become so much of an issue in today's world that a hospital's accreditation is also dependent upon it. The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) has published a set of standards that require accredited facilities to develop an emergency preparedness plan. The commission further requires that facility staff be educated about the plan and possess the skills and responsibilities they would need if called upon to implement the plan.

The Accreditation Association for Ambulatory Health Care also requires an emergency plan that addresses both internal and external emergencies. It states that the facility must have the necessary backup equipment, trained personnel and procedures to carry out the plan if necessary. Increasingly, "trained personnel" includes nursing.

The building blocks of security

Nursing informaticians aren't the only ones accountable for data. While nursing informaticians may indeed be responsible for data *security,* all nurses have a strong responsibility for data *integrity.* Integrity refers to accuracy and timeliness of information: Have we recorded doctor's orders exactly as stated? Did we remember to document medication immediately after its administration? Have we entered data into the correct patient chart so the information exists for other staff members who need it?

Data security, on the other hand, has two main components:

1. *Privacy*. Data must be protected from unauthorized access.
2. *Preservation*. Data must be protected from tampering and potential destruction.

As caregivers, nurses must understand these issues, as vandalism to or loss of data can have a negative impact on quality of care. Nurse managers may also be called upon by the IS department to help secure data within their specific departments.

Emergency plans that address data security must take into account the following elements of the information system's infrastructure.

- *Physical safeguards.* Where is the system located? What about data backup systems – are they onsite or offsite? Does the location provide some amount of protection from fire and/or water damage? Is it inaccessible to hospital visitors and other outsiders?
- *User authentication.* Who is allowed to use the system? How do they gain access to the system? How is unauthorized personnel kept out? Does the authentication process have built-in safeguards?
- *Access control.* What level of data can users access? Is there a "need-to-know" system in place that precludes users from accessing data not relevant to their jobs?
- *System management.* What is happening within the network? Are backups automatic backups or do staff members initiate them? How often is data backed up? Does the system provide alerts for attempts at unauthorized access?

While physical safeguards and system management are the IS department's responsibility and expertise, the other two – user authentication and access control – are areas nurse managers must be aware of.

The beast within: Preventing internal terrorism

Disasters stemming from unauthorized use of either the system or specific types of data are *internal threats,* not external ones. While Internet hackers may command the media's attention, the FBI's Computer Crime Unit reports that most acts of vandalism to data are inside jobs, performed by disgruntled employees with an agenda of their own – usually revenge.

One of the biggest disasters any hospital can face is loss of or damage to the patient record. Computerized patient records (CPRs) in particular may be more vulnerable to attack than their paper counterparts. As managers who supervise the nurses that have daily access to the CPR, we can take some amount of responsibility for preventing internal attacks, largely by developing an awareness of what *could* happen in a worst-case scenario. While no one wants to dwell on the negative, every information system has vulnerable spots and it's important to be conscious of what these are. Specific areas that nurse managers can become involved in to ensure data security include:

- *Security incident procedures.* If you become aware of even a small breach to security within your department, immediately report it to IS. Small incidents can lead to larger ones and may be the first sign that there's a weak spot in the system. Whenever possible, work with IS to help generate a response to the incident, including suggesting ways to make the system more secure within your managed area.
- *Training.* Make sure your staff is aware of, and complies with, HIM policies regarding passwords. Often, an organization's best defense is the offense of changing passwords often. Those who use the system should be informed that their compliance helps prevent breaches to security. You can also help to educate your supervisees about computer viruses and how to prevent their spread. When any new security policy crosses your desk, train your staff in its effective use. Take responsibility for offering periodic reminders about existing security policies.

- *Termination procedures.* One of the biggest threats to data security is an angry employee. When you have to terminate someone, plan for the worst and then take steps to prevent the worst from occurring – change combination locks, be sure all card keys or badges have been retrieved. Above all else, work with IS to be sure that the employee's user account is immediately removed from the system and from all access lists. Change passwords that are shared by a group of people.

All secure? Not likely

Ben Franklin might well have presaged life in the Information Age when he said, "He that's secure is not safe." Few would argue that electronically stored information is safer than paper from a host of potential destroyers. But even electronic data is only as secure as an organization's policies, procedures and plans.

###