

## AUTOMATED SYSTEMS MANAGEMENT:

# Ensuring the Integrity and Accuracy of Patient Data

by Steve Nelson, MS, RRT, CPFT

- You just ran out of disk space on the body-box computer, so you start deleting files. Some of the ones you recognize get copied to a tape.
- The pulmonary lab supervisor gets an overnight delivery with a CD-ROM from the manufacturer of her spirometer. The instructions read, "Insert into drive and click on UPDATE."
- An RT student working in the staff library grabs a disk from his backpack to save the results of an online search. Unknowingly, the disk contains a virus that scrambles the registry information, then deletes data on a network-connected drive in your department.
- A former employee happens to be visiting in the hospital. While there, she walks by an unattended records terminal. She remembers her old access code, tries it, finds that it still works, and decides to check out a couple of random patient records.

Each of the above scenarios illustrates a potential data management problem in a hospital department. Whether data is stored or acquired on a computer, or simply hand-written on a standard form, ensuring the integrity and accuracy of data is one the

most important functions in a health care setting.

Data management can be separated into several categories. When referring to automated systems, policies should include record retention, security, backups, and program revisions.

## Record retention

Any test results obtained from a lab need to be safely retained for a period of time. Unfortunately, there is no universal rule to follow. Joint Commission on Accreditation of Healthcare Organizations requirements in section 6.1 of the Information Management chapter state: "The hospital determines how long medical record information is retained, based on law and regulation..."<sup>1</sup>

The American Health Informatics Management Association has adopted the policy illustrated in Table 1.

To further confuse matters, states and federal agencies have their own regulations. For example, Washington State requires keeping inactive records of minors for three years after they reach age 18.<sup>2</sup>

New Mexico requires those same records to be kept 10 years, or one year after reaching 18, whichever is greater.<sup>3</sup> Federal regulations for pulmonary function testing of workers exposed to asbestos require keeping records for 30 years after an employee leaves a company.<sup>4</sup>

Individual institutions even have rules. Indiana University Health Center publishes the following on their web site: "It is the policy of the Indiana University Health Center to destroy medical records that have remained inactive for eight years." There is an additional consideration for automated systems. If data is to be

**Table 1. Medical Record Retention Policy of the American Health Informatics Management Association**

<b>Record Type</b>	<b>Retention Period</b>
Adult Medical Record	10 years after most recent encounter
Minor's Medical Record	Until age of majority plus statute of limitations
Diagnostic Information	5 years for images
Master Patient Index	Permanent

kept available for 10 years, changes in technology come into play. Until a few years ago, most desktop computers were sold with 5 1/4" floppy disk drives, and backups were commonly written to QIC tape car-

tridges. Both of these features have virtually disappeared.

A functional version of the appropriate hardware will need to be kept in a "museum" as long as there are computer media requiring it to gain access to data. The ability of the media itself to retain information is also limited. Floppy disks are considered to have a useful data storage life of three years, tape cartridges from five to eight years, and various CD formats from 10 to 25 years. Data stored on these media need to be refreshed or transferred to new media on a regular basis.<sup>6</sup>

**Security and confidentiality**

The Joint Commission requires that "Records and information are protected against loss, destruction, tampering, and unauthorized access." Most data can be easily protected in computers using password protection programs. Passwords should not be considered a nuisance; try to avoid writing them on notepads beside the computer. Do not use generic log-in accounts like "pftech." Most



unauthorized access to systems can be prevented using passwords that are not easily guessed, such as your name spelled backwards, the room number, or your birthdate.

Computer viruses can cause corruption, alteration, or loss of data. These simple measures can protect a department's computer system:

- Scan all floppy disks before they are used. The source of all software should be known before installing it.
- Remove any software that is not necessary. If network connections are not being used to share data, remove them.
- When an employee leaves, voluntarily or otherwise, be sure that your exit process includes deleting or disabling any departmental access accounts and informing other departments that may have granted access to the employee that they should do the same. If a hospital-wide information system is used, contact that department as well.

### Backups

All hard disks crash, but this doesn't have to be catastrophic. Establish a regular backup schedule and follow it. Timely backups will allow a computer system and its data to be returned to a known status with minimal effort.

Backups should not be confused with long-term storage. If backups are mistakenly used for storage, they will need to be kept for as long as the data may be needed. Maintaining a museum of old computer systems and programs is not a productive use of time.

## references

1. Joint Commission on Accreditation of Healthcare Organizations. (1997). *Comprehensive accreditation manual: The official handbook*. Oakbrook Terrace, IL: Joint Commission.
2. Washington State Legislature. (1999). *RCW 70.41.190 Medical records of patients — Retention and preservation* [Online]. Available: <http://search.leg.wa.gov/>.
3. New Mexico State Records Center and Archives, Records Management Division. (1999). *General retention and disposition schedules*. [Online]. Available: [http://www.state.nm.us/cpr/records\\_grds.htm](http://www.state.nm.us/cpr/records_grds.htm).
4. Harber, P., Barnhart, S., Boehlecke, B.A., et al. (1996). Respiratory protection guidelines [Official statement of the American Thoracic Society]. *American Journal of Respiratory and Critical Care Medicine*, 154(4, Pt. 1), 1153-1165.
5. Indiana University Health Center. (1999). *Health center medical records retention policy* [Online]. Available: <http://www.iuinfo.indiana.edu/homeages/0131/0131text/digest.htm>.
6. The PaperCom Alliance. (1999). *Media longevity: Are we losing the preservation fight?* [Online]. Available: <http://www.papercom.org/disks.htm>.

### Programs and revisions

Updating software is not a trivial matter, especially if it involves a change in methodology. Validation of the software methods should be performed by the manufacturer and verified by the lab. The vendor should document that test results using the current software will match test results obtained after the upgrade or it should explain the expected differences.

Decision-making software algorithms, such as those used to classify pulmonary function tests and grade severity of impairment, need to be accessible in a human-readable format. This can usually be accomplished by keeping reprints of the reference articles from which they were derived.

Finally, by the time you read this, it is probably too late to start worrying about any prob-

lems resulting from incorrect date calculations related to Y2K. Just be sure that your patients don't suddenly start showing up with negative ages in January 2000. 🙄

Steve Nelson is a computer consultant in Overland Park, KS. He also teaches spirometry testing and performs employee health screenings.

See the  
“Tools of the Trade”  
Column on the  
“Table of Contents”  
in this issue for  
additional resources  
on  
this topic.