AUTOMATED SYSTEMS MANAGEMENT:

Ensuring the Integrity and Accuracy of Patient Data

by Steve Nelson, MS, RRT, CPFT

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.”

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.

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, back-ups, and program revisions.
New Mexico requires those same records to be kept 10 years, or one year after reaching 18, whichever is greater. Federal regulations for pulmonary function testing of workers exposed to asbestos require keeping records for 30 years after an employee leaves a company.

Individual institutions even have rules. Indiana University Health Center publishes the following on their website: “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 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 cartridges. 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.

### 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.”

---

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

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult Medical Record</td>
<td>10 years after most recent encounter</td>
</tr>
<tr>
<td>Minor’s Medical Record</td>
<td>Until age of majority plus statute of limitations</td>
</tr>
<tr>
<td>Diagnostic Information</td>
<td>5 years for images</td>
</tr>
<tr>
<td>Master Patient Index</td>
<td>Permanent</td>
</tr>
</tbody>
</table>

---

AARC Times  November 1999
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

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 problems 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.