# Securing the Company Jewels

## ELECTRONIC DATA AND IMAGE STORAGE

*By Jorge Sanchez, Jr.*

It isn't difficult to see the impact computers have had on the way companies do business. In a little more than a decade, offices have gone from having one or two computers to a computer on every desk, communicating with one another and interacting with the World Wide Web.

Once relegated to simple tasks, such as creating and maintaining spreadsheets, computer systems have become the backbone of every business organization, providing access to all forms of pertinent data and streamlining operations. As a result, the protection and retention of electronic data has become extremely important. In December 2006 the U.S. Supreme court amended the Federal Rules of Civil Procedure (FRCP) to detail the procedures for the disclosure, discovery, and use of electronically stored data belonging to an organization.

The regulations were set forth to protect both the individual and the institutions housing data. In a time when identity can be stolen as easily as a purse, it is imperative that electronic data be maintained in compliance with these regulations.

Data storage for medical billing companies is particularly important and falls under guidelines from HIPAA. In the event of data compromise, the billing company will be held liable for the data housed within its systems, regardless of whether the system is on-site or hosted remotely. Even without compromise, a billing company may be fined if it is found to be out of compliance with regulations. Failure to maintain a compliant and secure system can be catastrophic for a billing company and in a worst case scenario, cause it to close its doors.

Because all data storage is not the same, you need a thorough understanding of your data storage needs. This includes whether your data is raw data entered and stored into a computer system or whether it is electronic images (scanned and captured paper documents stored on a computer system or electronic storage media).

### HOW DO THE AMENDMENTS IN THE FRCP AFFECT YOUR COMPANY?

The FRCP does not directly regulate how electronic data must be stored and/or managed. It does, however, directly state the need for a document retention or data retention policy. This policy is specific to your company and will be the guideline that your organization uses to ensure that all electronic data stored in accordance with state and federal requirements. It is your protection should litigation be required. It is always a good idea to have legal counsel review your retention policy to verify that it encompasses all requirements.

The following example shows how a data-retention policy may protect your organization.

Let's assume your organization has in place a valid, verified, and working retention policy. A portion of this policy states that data pertaining to certain medical billing-related material is to be retained for no more and no less than seven years. Data reaching the term of seven years of age will be permanently deleted from the data system and removed from all backup media. From that point forward that data no longer exists.

Should your company be brought to litigation and the legal action requires presentation of medical billing data that is eight years of age, your company will be prepared. Elements of the amended FRCP shows that if electronic data is unavailable due to policy, and as long as the organization follows compliance, it is not to be held responsible for failure to produce the requested data.

### ELECTRONIC DOCUMENT STORAGE

After creating a retention policy, the next step is to determine how to store your document. The simplest method to ensure their security is to eliminate paper and store everything electronically. Here are some of the things to look for in a document storage company:

- Document imaging that converts paper files to electronic images, which are legally accepted as the original.
- Files that can be immediately accessed by authorized users via the Internet with enhanced search functionality.
- Files that are simultaneously viewable by multiple employees.
- The ability to directly import and expot Microsoft Word documents and images directly to and from online storage.
- Frequent backups delivered as CDs with electronic backups in two locations
- Users and security levels that can be assigned to each stored file cabinet.
- Search capabilities by client, patient, employee name, policy, medical record, employee number, company, carrier, vendor name or policy type

Nothing should be overlooked when transitioning to an electronic office. With careful consideration and due diligence your organization can ensure both your data and your organization is well informed and prepared. ▲

*Jorge Sanchez, Jr., is IT manager for eBridge Solutions in Tampa, FL. He can be reached at JSanchez@ebridge-solutions.com.*