

SOME OPTIONS FOR THE STORAGE AND DISPOSAL OF MEDICAL RECORDS

By Peter Dempsey

As hospitals, health-insurance providers, and related entities across the country endeavor to comply with new privacy and security standards promulgated under the **Health Insurance Portability and Accountability Act (HIPAA)**. There is growing interest in effective and efficient ways to manage protected medical records. Not the least of many concerns are the safe storage of such records and, once they become obsolete, their destruction. A brief overview of the equipment available to facilitate such storage and disposal may be helpful.

The pertinent federal regulation (45 CFR Parts 160, 162, 164) requires each covered entity to institute formal, documented policies and procedures that specifically address access to records, the disclosure, transmission, storage, and destruction of records, the fair handling of complaints, staff training, data backup, and other concerns. Although Section 164.530 (“Administrative requirements”) of the regulations states that a covered entity “must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information,” it does not specify any technologies.

Neither the “privacy standards” for paper documents nor the “security standards” for electronic records dictates specific means of compliance. However, the preamble to section 164.530 does cite a few examples of appropriate safeguards, such the locking of file cabinets that contain protected documents and the shredding of such documents prior to disposal. For electronic media, Section 164.310 (“Physical safeguards”) requires covered entities to specifically address “the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored” and to implement procedures for “removal of electronic protected health information from electronic media before the media are made available for re-use.”

Obviously, the equipment selected to carry out a HIPAA compliance plan will differ according to the nature and size of the business. Wisely allowing for such differences, the regulations require each covered entity to designate a “privacy official” to develop and implement its plan. Accountable for all of the entity’s privacy-related issues, this person will have to decide exactly which procedures and equipment will best prevent unauthorized, unnecessary, and inadvertent disclosure of protected information. For storage, this means locked office doors and cabinets, computer firewalls and passwords, etc. For disposal, to put it bluntly, it means destroying records to the point where no one can dig them out of the dumpster later and misuse them. Discarded medical information is often still confidential.

As for storage, cabinets and containers on the market today offer a wide range of security levels, for paper documents as well as for records on electronic media (magnetic tape or disks, CDs, memory cards, etc.). At one end of the spectrum are simple locking file cabinets. At the other are sophisticated, fireproof safes.

When records are destined for disposal, storage and disposal functions may overlap. Privacy officials may want to consider purchasing secure waste receptacles. At first glance some of these appear to be typical steel trashcans with hinged doors at the top, but their design prevents the removal of material even if they are turned upside down. For instance, a welded, curved chute permits the deposit of bound reports or thick stacks of paper while preventing arms from reaching in. The hinged top is lockable, of course.

Another type of receptacle looks like an attractive metal locker with a built-in file-cabinet drawer on top. Material can be dumped into (but not retrieved from) the "locker" below, the door of which has concealed hinges to discourage tampering. Inside, waste falls into a canvas bag with carrying handles, a rugged zipper, and a hasp for a small padlock.

When it comes to destruction equipment, the variety is even greater – much greater. Because of the variables and tradeoffs involved, a privacy official will probably want to put some thought into designing a comprehensive shredding program that is efficient for his or her particular facility.

Paper shredders are available in all sizes, speeds, horsepower, and capacities. Their cutting heads differ too, depending on the desired size of the shreds. Conventional strip-cut shredders produce strips that possibly could be pieced together later by unauthorized persons. Cross-cut shredders turn paper into small squares of varying sizes, depending on the model. Heavy-duty, high-volume shredders can destroy bound reports and large stacks of paper.

To illustrate some of the decisions that come into play when planning an institutional shredding program, the choices can be broken down into three basic arrangements:

Personal: Desk-side shredders, available on casters for portability, can shred roughly 6-20 sheets at a time. For offices with relatively few documents to destroy, the convenience of these models may obviate the need for pre-shredding storage containers. Shreds accumulate in plastic bags that can be combined with other trash.

Departmental: Larger facilities with more documents to dispose of may choose to install a more powerful shredder in every department or on every floor. Depending on horsepower and type of cutting head, these can shred roughly 20-50 sheets at a time. Instead of waste bags, some models have extra-large, wheeled bins inside, facilitating disposal to a central location. Where the

accumulation of shreds from multiple shredders would present a problem, a “briquetter” machine can be used to press shreds into dense briquettes, reducing waste volume by as much as 80%.

Centralized: For high-volume shredding, a single heavy-duty shredder may be the best choice. Capacities for this type range as high as 400 sheets at a time, so these machines have no problem destroying bound reports and thick stacks of paper. Balers can be attached to some heavy-duty shredders.

These alternatives are arbitrary; hybrid programs are common. Whatever shredder models are selected and however they are configured, it should be clear by now that a facility will need protocols for managing shredded waste, all the way to its final disposition. Some companies, including at least one shredder manufacturer, offer regular pickup of plastic bags, bins, bales, or briquettes, which are transported to landfills or recycling facilities.

Also on the market are powerful “disintegrators” that use rotary-knife systems to reduce high volumes of books, binders, paper bundles, and other bulk materials to tiny particles. Depending on the model, these machines even pulverize CDs, DVDs, floppy discs, microfilm, credit cards, ID badges, tape cassettes, circuit boards, etc., slicing them into indecipherable fragments at the rate of up to two tons per hour. The waste can be tailored to any desired particle size via interchangeable screens, through which oversize particles cannot fall until they are further reduced by the high-torque, two-stage cutting system. A disintegrator can be ordered with a conveyor belt, a noise-reducing enclosure, or a vacuum evacuation system that sends the particles through flexible tubing to a nearby bag, bin, or even an outdoor dumpster or truck.

Other machines, designed specifically for optical media, can completely remove data-bearing surfaces from CDs and DVDs. Because their “micro-machining” process leaves inner disc hubs intact, the hubs can be identified as absolute proof of destruction, eliminating the need for detailed logs and witnesses where certification of destruction is required.

Security may become an issue when a business donates old computers to a school or some other organization. In some cases, the old units are removed and resold by the vendor who installs the replacement computers. Most people are not aware that when a digital file is “deleted” the information actually remains on the computer’s hard drive or a formatted diskette, as do deleted e-mail messages and records of all online activity. These days it all can be recovered with sophisticated tools.

“Disk-wiping” software can prevent unauthorized recovery by overwriting entire drives/disks (or particular sections of them) before these magnetic media are discarded or reused. Overwritten areas should be unreadable, but some software packages are more thorough than others; look for a brand that meets or exceeds

the Department of Defense standard for permanent erasure of digital information (U.S. DoD 5220.22).

For absolute certainty in erasing magnetic media, there are several types of degaussers, which remove all recorded information in a single pass, allowing hard drives, diskettes, audio and video tapes, and four- and eight-millimeter data cartridges to be reused many times with no interference from previous use. One model is designed just for video cassettes. Hand-held degaussing wands erase both floppy and hard computer disks.

In conclusion, due to differences in size and mission, hospitals and other entities covered by the HIPAA regulations may implement different plans and make use of different equipment in order to safeguard the privacy and integrity of health information. Nevertheless, every entity must address the same issues, which include the storage and disposal of protected records. For both electronic and paper records, the variety of equipment on the market today enables a hospital or other entity to tailor its compliance to its own particular needs.

Peter F. Dempsey is president of Security Engineered Machinery (SEM). In addition to its business customers, SEM supplies destruction equipment to every American Embassy in the world and various U.S. military, intelligence, and law enforcement agencies. The company maintains a full-service engineering department that designs special products, such as the currency-destruction systems in use by the Federal Reserve Bank and other central banks; equipment for destroying "off-spec" or returned products in the pharmaceutical, medical-device, and food industries; and heavy-duty, high-capacity shredders for recycling applications. There are more than 100 authorized SEM service centers worldwide. For more information, contact Lisa Gauvin, Sales Representative, SEM, P.O. Box 1045, Westboro, MA 01581, TEL (toll free): 1-800-225-9293, FAX: 508-366-6814, www.semshred.com.