Computer Recycling: Are you Legally Prepared

Save to myBoK

by Joseph P. Harford, MS

As the healthcare industry continues to prepare for HIPAA compliance, two obstacles are emerging—the safe and legal disposal of outdated computer equipment and the digital or physical data destruction of patient information contained on them. This equipment comes in the form of computer monitors, hard drives, printers, copiers, and more. In the past, this equipment may have been placed into storage, donated to a school, or sent to the dumpster.

None of these methods of disposal address healthcare organizations' environmental or legal responsibilities. But how do you know if your organization is legally positioned to handle disposal of computer equipment? This article will address these concerns.

What Is Legal?

To determine if your organization is legally prepared in terms of computer equipment, three questions should be addressed:

- Does your organization have a plan in place for the removal and disposal of outdated computer equipment?
- Does your plan adhere to appropriate local, state, and federal environmental laws for equipment removal or recycling?
- Does your plan follow the appropriate local, state, and federal laws regarding the privacy of patient data that may still reside on the equipment in question?

The 1976 Resource Conservation and Recovery Act addresses the proper disposal of hazardous materials. Computer monitors contain an average of five to eight pounds of lead in the glass. Computer equipment also contains materials categorized as hazardous such as mercury, cadmium, and arsenic. Dumping large amounts of this equipment into a landfill is against the law. In summer 2002, the Environmental Protection Agency filed fines for the improper disposal of hazardous waste that included computer monitors. For more information on such fines, go to www.epa.gov.

It is estimated that by 2004 there will be 350 million obsolete computers in the US with no clear channel for removal, recycling, or disposal. This volume of equipment not only poses an environmental nightmare but also a challenge regarding the protection of privacy. Many states are attempting to enact legislation that will control the disposal of this equipment. Massachusetts and New Jersey have created a ban on dumping it into landfills. Pennsylvania will soon require a permit for companies that want to be involved with electronic recycling.

Protecting PHI

Although it is not directly addressed by HIPAA, it is obvious that proper recycling of computer equipment that contains protected health information (PHI) is just as important as following the guidelines for secure document storage and document destruction. The removal and recycling of computer equipment should be partnered with the need to properly and securely destroy PHI.

Healthcare organizations are aware of the need to work with a trustworthy document storage and destruction company. However, in many cases, the electronic source of all of these paper documents is forgotten. There have been numerous cases in which drives have not been properly "cleansed" and information has been inadvertently given away.

Destroying Data

Data destruction is not as simple and straightforward as "formatting" the hard drive of a computer. In fact, simply formatting the hard drive is in no way secure, comprehensive, or reliable. It is critical to implement responsible practices that consider the fiduciary responsibility of a healthcare provider to its patients.

The US Department of Defense has set forth standards for the reliable and secure destruction of both electronic and physical data that resides on a computer hard drive. In the absence of standards of this type, healthcare organizations may want to consider adopting these standards when completing the task of secure data destruction. It may be helpful to refer to the standards listed in the National Industrial Security Program Operating Manual at www.dss.mil/isec/nispom.htm.

Healthcare organizations may find the internal task of electronics re- cycling to be a daunting one and may decide that the identification, inventory management, destruction, and certification of private data should be left in the hands of reputable recyclers.

While it is always necessary to perform due diligence on a vendor, it is critical in this case in light of the potential environmental and confidentiality liabilities that organizations face. Ideally, an electronics recycler would perform both certified digital and physical data destruction services. Simply purchasing software or removing and destroying the hard drive is not adequate to protect an organization from an information breach.

The information that is solicited from a potential recycler or destruction vendor should be similar to that collected about the document storage or destruction vendor that may already be working for the organization. When choosing a recycling/destruction vendor, consider the following issues:

- landfill policy
- employee training
- background review and bonding
- data destruction practices and insurance coverage

Even with a vendor in hand, the liability associated with improper computer disposal or data loss ultimately remains with the accused institution. Make sure your organization is prepared.

Joseph Harford *(joseph@reclamere. com) is vice president of sales and marketing for Reclamere Inc., a company specializing in end-of-life services for electronic equipment.*

Article citation:
Harford, Joseph P. "Computer Recycling: Are You Legally Prepared?." *Journal of AHIMA* 74, no.3 (2003): 54.
