VENDOME GROUP, LLC
Healthcare Informatics Online

SHOP TALK

Data Disposal

Data security has become an important issue since the revision of HIPAA's privacy provisions.

by Brooks Hoffman

It is estimated that global spending on security software reached $50 billion in 2005. While most organizations have concentrated on preventing outside intrusions into their networks, there has been comparatively little attention focused on protecting information that leaves the organization on retired information technology assets.

Unauthorized disclosure of personal health information (PHI) in this manner may constitute a violation of HIPAA - resulting in fines of up to $50,000, as well as imprisonment for up to one year. In addition, the inadvertent release of sensitive data may violate a number of other recently enacted federal privacy laws - including the Fair and Accurate Credit Transactions Act and the Gramm-Leach-Bliley Act.

Violation of these laws can result in substantial criminal and civil penalties as well as significant negative publicity. In January, the Federal Trade Commission announced a consent judgment against consumer data broker ChoicePoint, Inc. (Alpharetta, Ga.), which admitted that the personal financial records of more than 163,000 consumers in its database had been compromised.

Under the terms of the agreement, the company would pay $10 million in civil penalties and $5 million in consumer redress to settle charges that its security and record-handling procedures violated consumers' privacy rights and federal laws. The settlement also requires ChoicePoint to establish and maintain a comprehensive information security program and obtain biannual third-party audits by an independent security professional for the next 20 years.

Here are some initial questions to consider when assessing the data privacy safeguards that govern your organization's IT asset retirement program:

- Have you put in place the necessary procedures and controls to check the efficacy of the entire data destruction process from transportation through actual

destruction? Is the process audited by a third party? How does your organization monitor chain of custody? Do you obtain photographic evidence to verify that the data has been destroyed?

- Does the potential resale value of the retired assets offset the potential costs of a breach of data privacy? In order to maximize information security, many organizations prefer to recycle all of their end-oflife IT assets regardless of residual value.
- Should you perform your data destruction activities in-house? There are two basic methods available: physical destruction and software destruction. Physical destruction involves either degaussing the storage media by using a magnet or physically deforming it in some way to prevent normal operation. Physical hard drive destruction equipment is commercially available from companies such as Shred-Tech (Cambridge, Ontario) or SEM (Westboro, Mass.). Software destruction involves overwriting the data by filling the hard drives with zeros. There are a number of commercially available software programs - including Eden Prairie, Minn.-based Kroll-Ontrack's “Data Eraser” and Mississauga, Ontario-based LSoft's “Active Kill Disk.”

Faced with competing internal priorities and limited resources, an increasing number of organizations have chosen to outsource the retirement of their IT assets. However, this decision may ultimately put the company at even greater risk if they rely on consignment organizations with no expertise in data security or sham recyclers that offer “free” recycling.

In evaluating potential asset retirement vendors, it is important to ask what physical and/or software destruction capabilities they have. All candidates should possess a baseline capability of data destruction that meets Department of Defense 5220.M standards. Other important questions to ask include the following:

- Do they undertake a sampling process and/or disk inspections via computer forensics?
- What kind of onsite security systems are in place at their facilities in order to ensure protection of equipment?
- Does the vendor maintain an errors and omissions insurance policy in the event that some data is accidentally disclosed?

Lastly, it is critical to assess whether the prospective vendor has your organization's best interests in mind - i.e. are they motivated to provide the appropriate services or are they simply looking to profit from a quick resale of the equipment being retired?

Managing the data security risks inherent in your organization's IT asset retirement program does not have to be difficult or expensive. However, it does require IT executives to: 1) Educate their organizations on the importance of maintaining information privacy, and 2) Develop and implement programs that effectively mitigate risk.

Brooks Hoffman is vice president, finance and operations, LifeSpan Technology Recycling, Newton Upper Falls, Mass.