

SelectShred News

JANUARY 2014



INFORMATION DESTRUCTION—SHREDDING PAPER AND BEYOND

In addition to shredding paper with confidential information for protecting privacy and fighting identity theft, individuals and businesses are also charged with a lot more than destroying paper in the digital age. Computer hard drives, copier hard drives, cell phones, optical media (CDs/DVDs), thumb drives, digital tapes, memory chips, and credit/debit cards all need to be physically destroyed to avoid retrieval of the information contained on these media.

According to an investigative report done in 2010 by CBS News, it was reported that *"Nearly every digital copier built since 2002 contains a hard drive — like the one on your personal computer — storing an image of every document scanned, copied, or emailed by the machine."* Many people understand that paper with confidential information, credit cards, and computer hard drives must be destroyed but many never think about the other media, like the copier hard drives that store personal or sensitive information.

Companies are charged with safeguarding all the confidential information in their custody. Regardless of the media that contains confidential information, the same level of accountability for protecting that information is expected due to federal privacy laws. When protecting information, it is important to think beyond shredding paper with confidential information to destroying other media containing sensitive information. Proper disposal of all media must be met.

HHS Settles with Health Plan in Photocopier Breach Case

Under a settlement with the U.S. Department of Health and Human Services (HHS), Affinity Health Plan, Inc. will settle potential violations of the HIPAA Privacy and Security Rules for \$1,215,780. OCR's investigation indicated that Affinity impermissibly disclosed the protected health information of up to 344,579 individuals when it returned multiple photocopiers to a leasing agent without erasing the data contained on the copier hard drives. In addition, the investigation revealed that Affinity failed to incorporate the electronic protected health information stored in copier's hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the hard drives to its leasing agents.

Source: U.S. Department of Health & Human Services. HHS.gov.

DID YOU KNOW? It is a company's legal responsibility to properly dispose of any sensitive information stored on its digital copiers. (Source: Federal Trade Commission.) Follow this link to learn more <http://www.business.ftc.gov/documents/bus43-copier-data-security>

Commercial

Call **772-463-3166** OR email **INFO@SELECTSHRED.COM**
SelectShred, Inc. ■ 7960 SW Jack James Drive ■ Stuart, FL 34997

Residential