CASE STUDY

Don't Make this Mistake! It can be very expensive

Secure Data Destruction services are not a commodity

After 6 years of service to a local community hospital we were notified by the purchasing department that our annual secure data destruction service agreement (SHE) would not be renewed. We were told that purchasing had entered into a "master purchasing agreement" with a purchasing service that provided discounts on the purchase of all types of health service commodities. The more money spent with this service the deeper the discounts. Computer recycling and hard drive shredding were an available service.

The hospital IT department had been very satisfied with our services and registered their concern with working with an unknown and potentially unqualified vendor. We made the point that we were a licensed NJ DEP electronic recycler as required by the NJ E-waste law and that we were also the only NJ licensed recycler that was a NAID AAA certified secure data destruction vendor which is an important "vendor due diligence" qualification when using a 3rd party vendor for HIPAA data security requirements.

Even with our long history with the hospital and unique regulatory compliance qualifications, purchasing over ruled the IT department because of financial considerations. We requested that the IT department review their asset disposal records contained in our "Compliance Library" project documentation archive and compare our documentation to the new vendor.

The new vendor turned out to be a large national paper shredding company that could provide onsite hard drive shredding and would subcontract out the computer recycling activity. The first major change the IT department noted was that they were required to palletize all of their to be recycled hardware and they received a bill of lading only showing the pick up of a pallet by weight. They then received a bill from the paper shredding company for the recycling project according to the total weight recycled. There was no individual serial number by model and manufacture equipment audit provided. In contrast, our onsite recycling service technician would collect, sort, inventory and package the to be recycled equipment at the hospital location and provide a detailed bill of lading identifying the number of each type of equipment picked up followed by a detail equipment audit. However, the most telling contrast between our services is that almost every recycling project we performed for the hospital we found hard drives still installed in computers. The hospitals policy was to remove

all hard drives from computers prior to recycling and individually accounting for the hard drives during the shredding process. This hard drive control function is fundamental to the HIPAA required data asset control system. Our secure handling of the discovered hard drives complied to their required documented chain of possession data asset control process.

A second concern was with the paper shredding companies handling of solid state storage devices. Solid state storage electronic circuitry is much smaller than the physical components of a hard drive and require that the shredding size must be no greater than ½". Most shredding companies utilize 1" to 1.5" width shredders. We are one of a very limited number of onsite shredding services that can shred to a 3/8" dimension as required by NIST. As a test, the IT department included a quantity of USB drives in a secure container to be shred by the paper shredder. Normally the paper shredder removed the secure container to their shred vehicle and scanned the serial numbers of the hard drives and provided the hospital with a certificate of destruction with the serial number list attached. When the inventory list for the test was presented no USB drives were even identified as being shred.

The IT department presented this evidence to the purchasing department supporting their contention that the paper shredder was not capable of meeting the Hospitals HIPAA security standards and requesting to reinstate our services. Purchasing challenged IT to provide cost comparisons between the two services. While IT had extensive detailed historical documentation to support our charges they were unable to determine the charges from the paper shredder because of lump sum project charges with no supporting detail. Based upon this information, purchasing reinstated our IT asset disposal agreements.

Government regulations require the maintenance of detailed auditable records proving your compliance. In the absence of these records you are assumed not in compliance and potentially fined. In the case of HIPAA data security non-compliance it can be a fine of up to $1.6M.

It became clear that any price comparison between our services and the paper shredders services was a case of apples to oranges. The paper shredders services were bare bones and not up to the standards required for regulatory compliance thus putting the hospital in potentially serious risk of HIPAA fines and resulting damaging negative publicity.