

JEFF DAVIES

FORMER RISK MANAGER

INDIANA BLOOD CENTER
INDIANAPOLIS, IND.**IN THE BLOOD**

A risk manager's fingerprint identity solution for an Indiana blood bank.

When the Indiana Blood Center decided to convert its donor database software to a new system, Jeff Davies, the Blood Center's former risk manager, recognized that his employer had a potential liability risk on its hands.

On its database, the Blood Center had been storing the Social Security numbers of its donors as well as other personal information. That confidential information represented a risk for the Blood Center. Davies knew that in the event of a data security breach, the Blood Center could be held liable and face significant losses.

In making the conversion to the new system, Davies realized it would be better for the Blood Center to stop collecting donor Social Security numbers.

The FDA, however, requires blood centers to positively identify each of its donors and one of the prime ways of doing this was through the use of the donor's Social Security number. The Social Security number also was used to prevent donors from being in the Blood Center's system under several names such as Bob and Robert.

Davies came up with an elegant and revolutionary solution that eliminated the risk associated with storing donor Social Security numbers on his employer's database.

To positively identify donors, instead of using Social Security numbers, Davies proposed the idea of using fingerprint scans. Donors simply place each of their index fingers on a low-cost sensor that is connected to a Web browser and they are positively identified out of the over 500,000 donors the Blood Center has on record.

Software developed by BIO-key International uses that fingerprint data to develop a unique mathematical template, something like a bar code.

"This lets them stop storing Social Security numbers, which is a liability risk," said Jim Sullivan, director of sales at Wall, N.J.-based BIO-Key. "This is a great solution to a big problem. It was the first time it was done in a blood center," he said.

The fingerprint is a unique identifier and cannot be lost or forgotten like donor ID cards, which have been used by some blood centers. Replacing lost donor ID cards can be costly and donor ID cards are not foolproof.

For donors, meanwhile, the fingerprint scan eliminates the hassle of having to carry around another card in order to be able to donate blood.

Sullivan said that the Red Cross is now interested in using this technology to identify donors and several other blood centers are also considering the idea. The idea of identifying people with fingerprint scans makes a lot of sense for other businesses as well, such as banks and insurance companies.

One reason blood centers and other organizations had not adopted this technology sooner was because of perceptions that the technology was not reliable.

But Sullivan said there have been big improvements in the technology over the last few years and also points out that the software provided by his company is far more advanced than the software that is more widely distributed to general public.

It also helps that the BIO-key software is compatible with a number of different fingerprint scanners or readers, Sullivan said. Those readers are relatively cheap and many computers are now coming with them already installed by the manufacturer as part of the package.

"Some people don't believe in the technology, but they've refined it over the years," Davies said.

The Blood Center's ability to attract donors depended on finding a way to positively identify donors while protecting their confidential information. Donor confidence in the security of their information was crucial.

By investing in the technology of finger scanning, the Indiana Blood Center went above and beyond what any other center has done in this important area.

—By Patricia Vowinkel