

# California Pacific Medical Center Fingers Compliance

California Pacific Medical Center is one of the largest private, not for profit, academic medical centers in Northern California. It was recently ranked among the top 50 hospitals in America in a nationwide survey, and in 2001 was dubbed “The Healthiest Hospital in America” by Natural Health magazine. As CPMC began to focus on HIPAA compliance, they researched various approaches to secure their IT infrastructure while maintaining ease of use. They discovered that deploying fingerprint biometrics best met their needs for a user friendly, secure, identity foundation. And they found a way to fit it into their existing infrastructure without large disruptions.



---

## CPMC embarked on a project to have single sign-on across its systems coupled with strong user authentication.

---



**C**alifornia Pacific Medical Center (CPMC) traces its origins back to the 1850s, when the German General Benevolent Society opened a free clinic in a rented house on Mission Street in San Francisco. From this humble beginning grew the American West's first medical school in 1857, and first Nursing school in 1880. Medical technology firsts accrued as well, with the first iron lung west of the Mississippi in 1928, the first dialysis unit in Northern California in 1961, and the first CT scanner west of the Mississippi in 1972 among others. In the 1990s, California Pacific Medical Center was formed from the merger of Pacific Presbyterian Hospital and Children's Hospital of San Francisco. Later, Davies Medical Center joined CPMC which is now affiliated with Sutter Health.

California Pacific Medical Center has three hospitals, with over 1,250 beds and serves more than 200,000 patients annually. It provides a wide variety of services including acute hospital care, post-acute care, home care, outpatient medical care, and preventive, complimentary and educational services. In addition, CPMC provides professional education and biomedical, clinical, and behavioral research.

### HIPAA Meant Changes

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) placed requirements on health care organizations and their IT infrastructure to secure patient data and know who has access to it – to protect patient data. CPMC's patient focus is evident in the words of their CIO, Jerry Padavano, who said, "People tend to see HIPAA as

a nuisance, but I think it supports us. Without it, the extent of attention paid to privacy today wouldn't have happened. It's all about the patient. If we can prevent patient information from escaping and ensure their data is secure, that makes it all worthwhile."

As part of addressing HIPAA compliance, CPMC embarked on a project to have single sign-on across its systems coupled with strong user authentication. According to CPMC's Director of Technical Services, Brandon Williams, this began with a conversion to using Active Directory for their network authentication and authorization. "We're a Windows environment," said Williams. "We were on NT4 with Sutter until late 2002, but by early 2003 our Active Directory infrastructure was up and in place."

The AD infrastructure gave CPMC the ability to implement authentication, and thus auditing, to the user level, but changes in how employees used the systems were also required. "One of the things that we were not doing that we would consider best practice, and thus compliant with the HIPAA regulations, was unique IDs," said Williams. "Users logging into the windows PCs were not using unique user IDs, they were using a generic or group user ID. That blows your auditing capability."

A process conversion to unique logons also promised more user convenience, in addition to compliance. "If we introduced unique logins, which meets our auditing requirements, it also helps us automate a lot of things," said Williams. "If we can identify users upon login, we can run login scripts and some other

nice stuff." Implementing unique passwords, however, would not be without real world complications. "To do that means that [each user] has to have a user ID and password," said Williams, "and now [they] have got to remember that user ID and password." "Many of our clinical people were not that skilled in using computer terminals," said project manager John Kirkwood. "We needed to find a way to get them access to the PCs in a friendlier and more efficient and more secure way."

### The Search Begins

"We were looking for something that could help us automate that user ID and password function requirement," said Williams, "but something that would fit within our existing infrastructure. We wanted something that could preferably tie back into Active Directory because we don't want to manage another user database. We wanted to keep that same user database yet have it be fully compliant."

Their search quickly narrowed to RFID badges and readers and fingerprint biometric readers. "The RFID we were looking at, AKA proximity device or smart card, required a back end database server," said Williams. "And that requires extra infrastructure and support of that infrastructure. The other problem with the proximity devices is that it's more hardware. I don't think we've completely ruled out the wireless ID badge at this point, but we decided to put all of our focus and attention on the fingerprint reading device because it was a lot less technology that we had to put out there on the floor."

The search for fingerprint biometrics then focused on the infrastructure

---

**“A lot of fingerprint products require SQL servers and other back end databases. We wanted to try and stay away from that.”**

---

impacts. “A lot of fingerprint products require SQL servers and other back end databases,” said Williams. “We wanted to try and stay away from that. We also wanted something that met our price point. We wanted a device that itself met HIPAA requirements, meaning we don’t want it doing clear text user ID and passwords, etc. And we wanted something durable. We beat on about four different types of fingerprint readers, dropping stuff on them, dumping chemicals on them, hitting them with hammers, whatever, to try and find the one we saw would hold up the best in a clinical atmosphere.”

Their search narrowed to the Digital Persona fingerprint system as meeting the greatest number of their requirements. “The Active Directory database is all you need,” said Williams. “There is a small executable that gets run on all your AD controllers. We have across our organization a one site configuration in Active Directory, and it worked really well with the way we replicate AD controllers. Digital Persona has paid attention to what Microsoft has said to do when you are working with AD so you don’t run into anything really proprietary like you do with other products.”

“The [workstation] device is a fingerprint reader with a cable attached to the USB port,” said Williams. “It met all the price points, which is another big thing we cared about, and it also held up really well in the test lab through environmental stimuli and testing.”

## The Pilot Deployment

The rollout began with lab testing followed by a pilot deployment. “We start-

ed the testing in December 2003,” said Williams. “The lab testing and the technical testing on the AD side was all done first. So before any users saw it, there was about two weeks of testing.”

For the pilot deployment, about 80 PCs in the business office were chosen. This choice was made because the business office was located near the IT department, and also because there would be no clinical impact as CPMC learned from this pilot deployment. “One of the things that we saw in our own testing was that you’ve got to go through a registration process,” said Williams. “You’ve got to get everybody’s fingerprints in the system. So for our pilot, we brought in resources to go desktop to desktop and help register people. Because we really wanted to get any and all feedback that we possibly could out of that pilot, that person walked them through the registration process and had them test it a couple of times before we left them. We also were looking at [the] adjustments you can make in the software for margin of error, to make sure that their fingerprints were hitting each time they hit the reader.”

That pilot took place during the first weeks of 2004. “[It was] very well received in the business office,” said Kirkwood. “They understood what we were trying to do and they appreciated it.” Then it was time to start a rollout to the clinical areas of the medical center.

## The Larger Rollout

“When we went into the clinical areas it was also received really well,” said Williams. “There were some questions about infection control and the fact that

people are touching the devices, but they touch the mouse and the keyboard too so we were able to avoid having to go into that further once we tied it in with the other peripherals on the machine. For the single use PCs in the clinical environment it’s worked fine – inpatient therapy offices, genetic counselors, stuff like that where it’s a single user PC.”

## Process Change Reveals Issues

Multi-user PCs, however, presented a different problem – a problem that had nothing to do with the fingerprint authentication, but one that had to be addressed and solved. “In our high impact clinical use areas we have a lot of people using a lot of different PCs throughout a shift,” said Williams. “We have situations where you’ve got different people there on different days. Nursing is probably the biggest challenge. The problem is the time it takes to close down a Windows session and reopen a Windows session in those environments. Meeting with the nursing staff, the nursing administration group, and some of the other department directors, we were finding that the Windows log on time is just too long and it’s unreasonable that a user is going to walk up to a machine, do what they are doing and log out. It doesn’t really fit within their work flow.”

Searching for a way to gain compliance without creating a bottleneck, CPMC examined their options. “The application layer authentication is where we get our security,” said Williams. “From a HIPAA perspective, however, we have network shares that are tied to that net-



---

**“We often see a correlation or a dip in our patient satisfaction with a big software product rollout. We didn’t see that with this implementation.”**

---

work logon and here we are adding generic accounts to that. We need to move all of the employees onto a unique ID and password sign on procedure, but it doesn’t work within the work flow because Windows takes so long to log on and log back off. It’s not so much a problem for physicians, it’s more the nursing staff, because they are bouncing around looking up information so often in so many different areas.”

### **Finding an Answer**

To address this problem, Digital Persona is working with CPMC to create a software solution they call the Digital Persona Pro Kiosk. This software will allow people in a multi-user environment to share a generic Windows logon, but have unique indi-

vidual application logons. It is based on a timeout, so as a user leaves the PC it will automatically lock, ending that session. Then any other user that’s approved to have access to that PC under the generic Windows logon can put their fingerprint down and unlock the PC, creating a new application layer session.

Since the sessions are activated through AD, file access policy can switch without a Windows logoff and re-logon. This allows user context switches on a shared PC to happen rapidly. “We’re really excited about that product,” said Kirkwood. It’s going to give us the accountability that we need so we will know who is on the computer and when, and what they are accessing. But

it will still give our users easy access to the computer.”

To date CPMC has rolled out fingerprint authentication to over 1,500 of their 2,500 PCs. They are testing the Kiosk product and will roll out to the remaining multi-user areas as soon as they are satisfied it has solved their work flow problem. “It’s gone very well,” said Kirkwood. “It’s been a good deployment. CPMC is a not for profit, but we are a business like any other business and we look at our customers the way any other business does. We are constantly looking at patient satisfaction scores and we [often] notice that we can see a correlation or a dip in our patient satisfaction with a big software product rollout. We didn’t see that at all with [this] implementation.” ■