BioID fingerprint identification system
The next generation technology

Executive summary
The BioID fingerprint identification system on the Pyxis MedStation™ 4000 system includes biometric sensor technology that provides reliable authentication and identity verification in healthcare settings, accommodating multiple environmental and demographic variables. In this technical whitepaper, we will provide an overview of biometrics applications in healthcare, a brief discussion of how biometrics work, an overview of technical challenges for biometrics in healthcare settings and a thorough discussion of the third-generation biometric solution for the BioID fingerprint identification system.

Biometrics applications in healthcare
Biometrics play an important role in healthcare applications, especially when there is a need to control access through positive identification of authorized users. Biometrics also facilitate operational efficiency in healthcare by providing quick and easy access—reducing costly workflow interruptions that occur when passwords are forgotten or access cards are misplaced. Pyxis medication dispensing technologies were the first automated dispensing devices to widely deploy a biometrics solution to meet the needs of the challenging healthcare environment. Today, millions of Nurses access secured systems using BioID to care for their patients every day.

Biometrics overview
Biometric systems provide a means of verifying identity by collecting information about unique human characteristics and comparing that information to previously-submitted data. BioID incorporates a biometric sensor that collects information about users’ unique fingerprints and a matcher that facilitates decisions on whether access should be granted to the user based on data collected from the sensor.

The user places a finger on the external surface of the sensor, or platen, and relevant information is quickly extracted and transformed into a digital representation of the user’s fingerprint, or template. A template is not an image of a fingerprint, and fingerprint images cannot be restored from the encoded templates.

The user’s template is compared to the reference template the authorized user provided during an initial enrollment process. If the two templates match, the user is granted access. The entire process, from finger placement to match result, takes place in approximately two seconds with the BioID fingerprint identification system.

Understanding biometric performance
In order for a biometric deployment to be successful, the system needs to be able to quickly and reliably accept authorized users and reject unauthorized users. The two most common metrics for assessing biometric performance are the false accept rate (FAR) and the false reject rate (FRR). FAR measures the number of times the system allows access to someone who is not enrolled in the system. A high FAR exposes the system to security risks. FRR measures the number of times an authorized user is not recognized by the system. A high FRR creates hassles for authorized users who must try again or use an alternative method of gaining access.

The success of a biometric deployment also depends on how many authorized users can actually use the system. Failure to enroll (FTE) measures that portion of the authorized population that cannot use the system because the sensor cannot read their unique biometric information. These people will be unable to enroll in the system because the system will never recognize them. The failure to acquire (FTA) rate measures the number of times a sensor does not collect any biometric data at all. A high FTA rate slows system throughput.
Bringing biometrics to healthcare: the challenge

A sensor’s ability to collect usable data can be influenced by various external conditions, including demographic variables, users’ skin conditions, environmental variables and throughput requirements—making healthcare a particularly challenging environment.

- **Diverse user population**: Demographic variables such as ethnicity, sex and age all affect biometric performance and the diverse user population in healthcare has historically presented a challenge to conventional biometric systems.

- **Hand washing protocols**: Hospital policies require frequent hand washing and sanitizing for Nurses and others who come into contact with patients. Such users commonly have either very dry fingers or overly moisturized fingers. Both conditions can negatively impact an individual’s ability to enroll or use a fingerprint biometric system.

- **Environmental conditions**: Hospitals are often kept cool and dry. This type of environment, especially when combined with frequent hand washing, can result in dry, cracked fingers. Ambient fluorescent lighting can affect a sensor’s ability to capture a usable image. Hospital-approved disinfectants and moisturizing products can degrade sensor performance by damaging the data collection area of the sensor or interfering with the sensor/finger interface.

- **Throughput requirements**: Healthcare workers typically have time-critical duties and are susceptible to rushing through a biometric authentication process, which can affect the quality of data that is collected for future matching processes. In addition, all users may have variable finger placement or finger pressure on the sensor.

A successful biometric access system in the healthcare setting must maintain high biometric performance for each of these industry-specific challenges. Failure to reliably and efficiently authenticate the user places a burden on the staff, leading to unnecessary user frustration, a reduction in efficiency and poor adoption rates—reducing overall system security.

Conventional technologies fall short

The interface between the sensor and the surface of the finger is the primary vulnerability point of conventional sensors. Conventional fingerprint sensors fall into two main categories: semiconductor sensors and optical sensors. A new class of biometric sensor that relies on multispectral imaging will be discussed in the next section.

The two most common types of **semiconductor sensors** use small silicon arrays to measure either the difference in capacitance caused by contact of fingerprint ridges with the sensor, or the difference in radio frequency signals returned by the ridges and valleys of the fingerprint.

The fragile silicon array in semiconductor sensors is directly exposed to the environment and is susceptible to damage. Capacitive sensors don’t work well when the skin is very dry, and both capacitive and radio frequency sensors fail when the sensor surface is wet. Both capacitive and radio frequency sensors measure the surface features of the skin only, resulting in reduced performance when the features are worn or absent.

Semiconductor sensors are widely used for commercial applications where size and price point are the primary considerations. However, their fragility and unreliability make them inappropriate choices for secure healthcare applications.

**Optical sensors**, typically with a glass or acrylic platen, are configured to look for the presence or absence of total internal reflectance (TIR), which is the phenomenon whereby the interface between glass and air acts like a mirror at certain angles. The points of contact between the skin and the platen are imaged.

Conventional optical sensors are very susceptible to non-ideal skin conditions. In particular, if the skin is too dry or does not make good contact with the sensor, the performance is severely degraded. This difficulty with dry fingers can be addressed with a special coating on the platen that improves the quality of contact between the finger and platen. However, this coating is vulnerable to scratching and erosion from cleaning products that are commonly used in hospital settings.
Both of these conventional technologies—semiconductor and optical—have inherent vulnerabilities that make them unsuitable for the healthcare environment. In large-scale deployments or adverse environments, the overall biometric failure rates can be as high as 20% for semiconductor or optical sensors.

**BioID third-generation biometric solution: Lumidigm® technology**

To address the shortcomings of conventional fingerprint technologies, Lumidigm technology—multispectral imaging—was chosen for the BioID fingerprint identification system. This technology was specifically designed for and is uniquely suited to difficult application environments, such as healthcare settings.

**Multispectral imaging technology**

An important characteristic of fingerprint ridges is that their structure descends beneath the surface of the skin. Multispectral imaging collects information about the sub-surface fingerprint in order to augment available surface fingerprint data. Unique biometric data is collected under a variety of optical conditions: different wavelengths of visible illumination light, different polarization conditions and different illumination orientations. The varying optical conditions illuminate the skin at different depths, resulting in information-rich data about the surface and sub-surface features of the fingerprint.

The imager will collect data from the finger even if the skin has poor contact with the sensor (e.g., is dry, wet or contaminated with hand sanitizers and moisturizers). Multispectral sensors also have an uncoated glass platen that resists damage from harsh cleaning products.

**Meeting the healthcare challenge**

BioID with multispectral biometric technology was deployed in hospital settings in late 2008. Biometric performance has been enhanced in the following ways:

- **Lower FRR:** Multispectral sensors are less sensitive to variable conditions and poor sensor/finger contact, resulting in higher user satisfaction with BioID.
- **Lower FTE:** People who cannot use conventional sensors have no difficulty using the new BioID.
- **Lower FTA:** More people can successfully verify their identity using BioID on the first try.
- **Lower FAR:** The sub-surface capability of multispectral biometric sensors means more relevant data is collected, reducing the possibility that the system will mistake one user for another—enhancing security.

Tomball Regional Medical Center, a 357-bed hospital in Texas, dramatically increased user enrollment. Many users were previously utilizing alternate methods of authentication because they either couldn’t reliably use the system themselves, or they observed that other users had difficulty. With the third generation BioID, biometric performance skyrocketed, increasing reliability, convenience and security along the way.

“Before upgrading to the Pyxis MedStation 4000 system, only about 50% of staff was using BioID—now we have 100% compliance, which has greatly enhanced system security. It even works for users with skin issues like eczema.”

- Margaret Osburn, Pharmacy Informatics Project Manager, Tomball Regional Medical Center

**Conclusion**

Biometrics has a significant role to play in healthcare. The BioID fingerprint identification system provides reliable, secure, robust and easy-to-use biometric fingerprint authentication to the healthcare industry. BioID with multispectral biometric technology is the only biometric access solution in the industry that solves the special problems commonly found in the healthcare environment.