

4Sight Labs Calls for U.S.-Based Standards to Protect Biometric Data in Correctional Facilities

Correctional technology providers should meet higher standards for data residency, access, ownership and security.

TEMPE, AZ, UNITED STATES, September 15, 2026 /EINPresswire.com/ -- As correctional agencies increasingly adopt biometric sensors, artificial intelligence and connected monitoring technologies, [4Sight Labs](#) is calling for stronger standards governing where sensitive information is stored, who can access it and how the technology protecting it is sourced.

4Sight Labs believes technology handling sensitive information collected from Americans in government custody should follow a simple principle:

U.S.-based technology. U.S.-stored data. Access limited to appropriately authorized U.S. personnel. No undisclosed third-party access or secondary use.

"If a technology company is collecting sensitive information from Americans in government custody, agencies should know exactly where that data goes and who can access it," said David Sanders, CEO of 4Sight Labs. "Government data should not pass through an unknown chain of foreign organizations, contractors or third parties."

Sensitive Government Data Requires a Higher Standard

Modern correctional technologies can collect significant amounts of sensitive information, including biometric measurements, movement, activity, occupancy information, video-derived information and safety alerts.

The federal government has increasingly recognized the national-security implications of foreign access to sensitive American information, including biometric, health and U.S. government-



Protecting biometric data in corrections requires clear standards for where data is stored, who can access it and where the technology comes from.



A database can be physically located in the United States while still being remotely accessible elsewhere.

Agencies need to understand both where their data is stored and who can access it.”

David Sanders, CEO of 4Sight Labs

related data.

4Sight Labs believes correctional agencies should apply that same level of scrutiny when evaluating technology operating inside their facilities.

Before deploying these systems, agencies should be able to answer:

Where was the technology developed, and where is it supported?

Is sensitive data stored, processed and backed up in the United States?

Can anyone outside the United States access the production environment or customer data?

Which affiliates, contractors or subprocessors have access, and why?

Can government data be used for research, commercial purposes, product development, or AI and machine-learning training without explicit agency authorization?

“Data residency alone isn't enough,” Sanders said. “A database can be physically located in the United States while still being remotely accessible elsewhere. Agencies need to understand both where their data is stored and who can access it.”

Raising the Standard Across the Industry

4Sight Labs is encouraging correctional agencies to incorporate U.S. data residency, U.S.-person access controls, third-party disclosure, cybersecurity testing, data ownership, deletion requirements and restrictions on secondary data use directly into technology procurements and contracts.

These principles apply across the rapidly growing range of correctional safety technologies, including wearable biometric systems such as 4Sight Labs' OverWatch® and AI-enabled, camera-based safety technologies such as OptiGuard®.

“We aren't proposing a standard that applies only to other companies,” Sanders said. “We believe these principles should apply across the industry, including to 4Sight Labs. When technology is operating inside a U.S. correctional facility and handling sensitive information, government customers deserve to know where that technology comes from, where their data goes and exactly who has access to it.”

About 4Sight Labs

4Sight Labs develops technology designed to help correctional and public-safety professionals

improve safety, situational awareness, documentation and operational accountability.

Its OverWatch® wearable technology provides continuous biometric monitoring for custodial environments, while OptiGuard® uses AI-enabled computer vision to provide contactless safety and welfare monitoring within correctional facilities.

For more information, visit 4SightLabs.com.

4Sight Labs Sales

4Sight Labs

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/942472079>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.