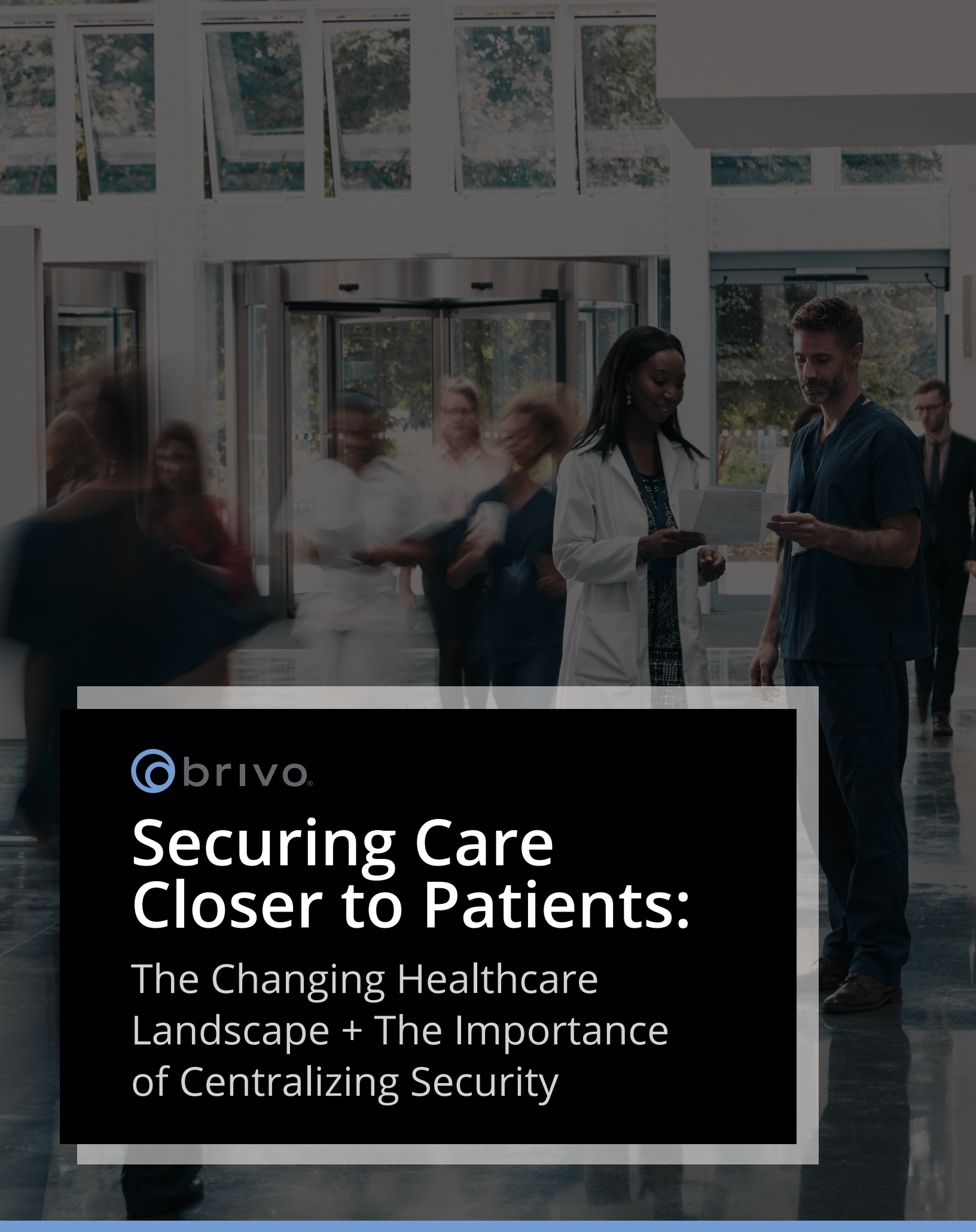

brivo

Securing Care Closer to Patients:

The Changing Healthcare Landscape + The Importance of Centralizing Security

The Importance of Centralizing Security

"Healthcare facilities are the most dangerous places to work in the U.S."

Hanover Research, Healthcare Security Spending, December 2022

You want patients to feel comfortable in your facilities and know they've come to the right place to seek care.

Your top priority is meeting the healthcare needs of the patients who come to your facilities. That means striking the perfect balance between warm and welcoming and safe and secure.

You want patients to feel comfortable in your facilities and know they've come to the right place to seek care. But protecting patients and staff – both their physical safety and the security of their private information – is vital to meeting your primary interest of being the best healthcare provider for your greater community.

We hear that's what keeps you up at night. Securing a healthcare facility is as complex as it is essential. According to Buildings.com, "Healthcare facilities are some of the trickiest buildings to secure properly."

And the Association of American Medical Colleges (AAMC) shared that the U.S. government reports that health care workers are "five times more likely to experience workplace violence than employees in all other industries."

Keeping Control Over Compliance

Beyond the trend of increased workplace violence to contend with, there is a need to keep controlled medications out of the wrong hands; a plethora of private and sensitive data to keep safe; expensive medical equipment and precious medical supplies to protect; and a list that goes on and on.

NPR reported that “many healthcare facilities still lack proper controls and security systems needed to spot drug diversion,” the technical term for medical drug misuse.

Beyond the trend of increased workplace violence there is a need to keep controlled medications out of the wrong hands.

"...many healthcare facilities still lack proper controls and security systems needed to spot drug diversion,”

A May 2023 story in MSSP Report discusses a recent Critical Insight Report analyzing breach data from the U.S. Department of Health and Human Services (HHS). According to the report, it was found that data breaches affecting healthcare providers declined in the second half of 2022. However, despite the decrease in the number of breaches, the report revealed a concerning trend - the number of individual records exposed in these breaches actually increased by 35 percent. This suggests that while the overall number of breaches may have decreased, the impact on individual data privacy and security has intensified.

The report indicates that while the number of breaches decreased in 2022, the exposure of individual records surged by 35%.

A healthcare worker in South Carolina was arrested in spring 2023 for allegedly stealing an electrocardiogram (EKG) machine, two Welch Allyn machines, and mobile devices worth more than $75,000, while two Michigan healthcare workers and a third person were charged in 2021 with selling $560,000 worth of stolen hospital supplies and equipment.

Of course, you must manage, rectify, and prevent all the above to not only fulfill your facilities' mission, but also meet compliance requirements for HIPAA, JCAHO, OSHA, SOX, and other government and industry standards.

There's, quite simply, a lot on your plate.

Growing Quickly to Meet Needs

We don't have to tell you, but the healthcare sector itself is expanding and evolving at a rapid pace.

From mergers and acquisitions and the addition of satellite locations to improve services...to an ever growing need to hire providers and support staff to meet the healthcare needs of a larger aging population...to more common dangerous weather incidents complicating the healthcare landscape...to the expansion in the use of artificial intelligence and other technologies...your job is not getting less complicated.

Forbes says "the number of older Americans [...] will continue to grow - peaking in 2030 at roughly 56 million adults - and the impact on our health system will be enormous."

According to the AAMC, "Hospitals around the country are indeed preparing for more frequent and severe weather events — from heat and hurricanes to blizzards and floods — through upgrades to their campuses, equipment, and emergency plans. In New York, walls arise on parts of the campus at NYU Langone Health to hold back floods. In Madison, Wisconsin, drones alert UW Health to clogged storm drains. In Omaha, staff at Nebraska Medicine strap hospital executives onto medical sleds to practice evacuating patients. In New Orleans, Ochsner Health has a fleet of boats and tall trucks to ferry staff, patients, and supplies during storms."

"the number of older Americans [...] will continue to grow - peaking in 2030 at roughly 56 million adults - and the impact on our health system will be enormous."
Forbes

How Can You Simplify Your Ever-Expanding Job of Securing the People, Assets, and Data Within Your Facilities?

Cloud-based access control is changing how healthcare organizations are centralizing and securing their facilities through opportunities to:

- Set a time schedule to automatically lock and unlock doors
- More easily meet compliance requirements and conduct and pass audits
- Open doors remotely and check if other doors are locked from a phone, tablet, or PC
- Eliminate the time and costs associated with rekeying a facility each time someone misplaces a key
- Review access events during investigations
- Track access to help prevent thefts
- Separate access between medical facilities
- Get reporting to confirm staff member, vendor and contractor access events
- Limit access to the vaccine cabinets to specific doctors and nurses
- Administer multiple sites from a single web interface
- Program access cards remotely in minutes
- Have more accurate access records and data that can be shared with other departments

"I got a call that a doctor wasn't able to get into the facility. All I had to do is grab my phone and open the door for him. Plus, I changed his access rights so he can get into his office permanently."

Director of Operations, Chancellors Ways Medical Arts Center (CWMAC) in Ontario, Canada

Integrating the Virtual and Physical Environments

For thousands of healthcare providers across North America, electronic and cloud-based access control are connecting with their corporate identity access management (IAM) solution to unify both the physical and digital access environments.

In many ways, physical security has lagged its cyber counterpart. Many organizations rely on legacy systems—typically on-premises, keycard-based, and facility-specific—for access control. These legacy systems are generally not integrated across access control, video surveillance.

Integrated virtual (cyber) and physical access management, also known as identity access management (IAM), gives healthcare facilities a unified view of all access points in a single location. There's no need to cross reference multiple systems, which can be confusing and time consuming.

IAM automates user management to eliminate identical entries in more than one system, ensure that user HR records are constantly up to date, and populate all user permissions and status changes throughout the entire digital and physical access environment.

An integrated solution also helps with maintaining regulatory compliance, plus compliance with security protocols and best practices, like making sure least-privileged user policies remain in place.

Likewise, combined identity and access data from physical and virtual worlds can be analyzed to better detect anomalous activity or behavior, more quickly identify security threats, reveal vulnerabilities in the security infrastructure, and simplify system audits.

Even better, combining identity management and physical access control with other physical security systems can give you an integrated 360-view of your facilities and networks.

Combined identity and access data from physical and virtual worlds can more quickly identify security threats, reveal vulnerabilities and simplify system audits.

Let Brivo Help

- Cloud-native solutions
- Data and auditability
- SOC2 certification
- Centrally managed access management
- Integration to video
- Compliance with new and emerging rules
- Automatic software updates
- Unlimited scale – not limited by site or server location
- Remote management of all facilities

"The Brivo system makes my job easier and frees me up for other things. With Brivo, it's easy to find out what we need; the system doesn't lie. It's very easy to manage and we can focus our time on providing quality care to our patients."

Facilities and Purchasing Manager, Adelante Healthcare in Phoenix, Arizona

We know the healthcare industry

We have done this work for over two decades

We can help you choose the right solutions for your organization's unique needs

ABOUT BRIVO

Brivo, Inc., created the cloud-based access control and smart spaces technology category over 20 years ago and remains the global leader serving commercial real estate, multifamily residential and large distributed enterprises. The company's comprehensive product ecosystem and open API provide businesses with powerful digital tools to increase security automation, elevate employee and tenant experience, and improve the safety of all people and assets in the built environment. Brivo's building access platform is now the digital foundation for the largest collection of customer facilities in the world, protecting over 450 million square feet of real estate across 60+ countries. Learn more at **www.Brivo.com**

Find out more about Brivo healthcare solutions at

visit brivo.com