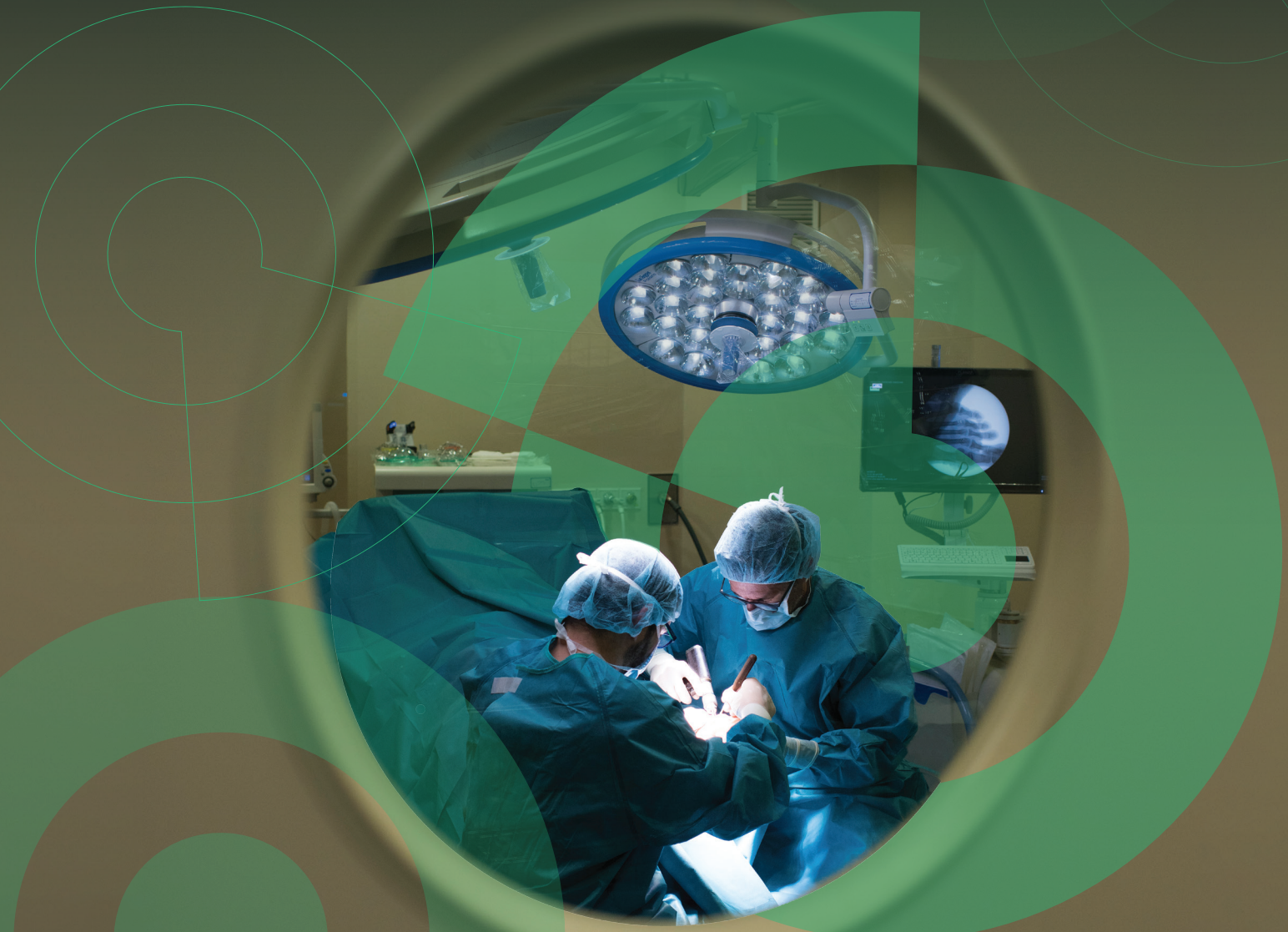
Green Security

Beyond the OR:

The Overlooked Vendor Risk Inside Hospitals



By Anna Ormiston, Green Security Vice President Customer Success & Operations

Green Security

Beyond the OR:

The Overlooked Vendor Risk Inside Hospitals

By Anna Ormiston, Vice President Customer Success and Operations at Green Security

Why credentialing programs must evolve to reflect how hospitals actually operate

For years, vendor credentialing in hospitals has centered on a clear and necessary priority: protecting patients in clinical environments. That has meant focusing on the individuals who enter the most sensitive spaces—particularly the operating room—where risk is immediate, visible, and tightly regulated.

Modern health systems rely on a broad ecosystem of third-party personnel. Environmental services teams, food and nutrition staff, biomedical technicians, maintenance contractors, and other service vendors move throughout facilities every day. They enter patient rooms, access restricted areas, and in some cases interact with systems connected to the hospital's broader infrastructure.

Yet many of these individuals fall outside the scope of traditional credentialing programs.

This creates a growing disconnect between how hospitals define vendor risk and where that risk actually exists.

> **Hospitals have built credentialing programs around the most visible risk, not the most common one.**

A Model That No Longer Reflects Reality

Credentialing programs were designed around clinical risk, and for a long time, that model was both logical and effective.

Hospitals prioritized vendors who were closest to patient care, particularly in high-acuity environments. Accreditation standards reinforced this approach, creating a structured system. But clinical vendors represent only a portion of the third-party population. The majority of non-employed individuals on site support operations, not care delivery.

These individuals were never fully integrated into the original credentialing framework; not because they were unimportant, but because they did not align with how risk was initially defined.

The Population Hiding in Plain Sight

Service vendors are embedded in nearly every aspect of hospital operations, yet remain peripheral in most credentialing strategies.

They include environmental services staff, food and nutrition teams, facilities contractors, biomedical technicians, and external service providers.

What makes this population challenging is its variability. Hospitals often know vendor companies, but not the individuals arriving on site.

Despite this, their level of access can be significant. They enter patient rooms, move through restricted areas, and interact with staff and infrastructure.

> **Organizations often know the vendor company. They don't know who is actually walking through the door.**

Where Current Approaches Fall Short

When organizations begin to extend credentialing beyond traditional clinical vendors, they tend to run into the same set of challenges. Most of these issues stem from how these programs were originally designed.

The first is visibility. Hospitals often have a clear understanding of which companies they work with, but far less clarity into the individuals those companies send on site. In many cases, the person performing the work is not identified in advance, and may not be the same individual who appeared the last time. That makes it difficult to apply a credentialing model that assumes a known and stable population.

> **A handwritten logbook is not a credentialing strategy.**

The second challenge is consistency. Vendor access is often managed differently depending on the department, the type of service, or the urgency of the request. A vendor who visits frequently may be partially credentialed, while another arriving for a one-time job may simply sign in at a desk or exchange identification for a temporary badge. These approaches create a record of presence, but they do not provide meaningful verification.

The third issue is that most credentialing remains static. Even when screening is performed, it is typically done at a single point in time—often at onboarding or contract initiation—with little visibility into what changes afterward.

Taken together, these gaps create a fragmented system. Some vendors are thoroughly vetted. Others are loosely tracked. Many fall somewhere in between. The result is not a lack of credentialing, but a lack of consistency in how it is applied.

The Risk Is Broader Than It Appears

One of the reasons this gap persists is that service vendor risk does not always present in obvious ways. It is diffuse, embedded in daily operations, and often only visible in hindsight.

Some of that risk is physical. Service vendors may enter patient rooms while patients are present or move through areas where vulnerable populations are being treated. Without appropriate screening and verification, hospitals may not have a clear understanding of who is present in those environments at any given time.

Some of it is operational. Vendors are frequently called in under urgent conditions. For example: when equipment fails, systems break, or repairs cannot wait. In these moments, access is often granted quickly, and processes designed for planned visits may be bypassed entirely.

And increasingly, some of it is tied to infrastructure. Vendors working on biomedical equipment, building systems, or facilities infrastructure may interact with assets that are connected to broader hospital networks. While their role may not be clinical, their access can still have downstream implications.

What makes this category of risk challenging is that it does not sit in one place. It spans safety, operations, and systems—and it reflects how hospitals actually function on a day-to-day basis.

> **The risk isn't who was approved six months ago. It's who is on site today.**

Why Static Credentialing No Longer Works

Traditional credentialing models are built around a fixed moment in time. They confirm that an individual met a set of requirements when they were first screened, but they offer little insight into whether those conditions still hold.

That limitation becomes more pronounced with service vendors.

These populations tend to be more dynamic than their clinical counterparts. Turnover can be higher. Roles can shift. Individuals may move between accounts or locations. A vendor who was cleared months ago may not represent the same level of risk today, but in many systems, there is no mechanism to detect that change.

This creates a lag between documentation and reality.

Credentialing, in this context, becomes less about current eligibility and more about historical compliance. And in an environment where access decisions are made daily—sometimes hourly—that gap matters.

What a More Modern Approach Looks Like

A more effective approach to vendor credentialing starts with a shift in perspective. Rather than asking how to extend existing clinical models to every vendor, it asks a more practical question: what level of oversight is appropriate for each type of access?

From there, a more modern model begins to take shape.

It is risk-based, meaning that requirements are aligned to the level of exposure associated with a given role. It is tiered, recognizing that a clinical representative, a recurring service vendor, and an ad hoc contractor should not be managed in the same way. And it is continuous, providing visibility that extends beyond a single point in time.

Just as important, it is grounded in operational reality.

Hospitals cannot function if credentialing processes create barriers to urgent work or introduce friction that leads to workarounds. The most effective programs are those that strike a balance—establishing clear, defensible standards while remaining flexible enough to support the pace and unpredictability of hospital operations.

The goal is not to apply more rules. It is to apply the right ones, consistently.

Case Study

Expanding Credentialing in a Pediatric Health System

> **Progress didn't come from solving everything at once. It came from aligning policy with how the hospital actually operates.**

One pediatric health system began to address this challenge after recognizing that its credentialing program, while effective for clinical vendors, did not fully reflect the population of individuals entering its facilities.

A significant portion of service vendors—particularly those tied to facilities, maintenance, and equipment—were operating outside a consistent framework. For an organization where safety expectations are inherently high, that gap raised important questions.

Rather than attempting a broad overhaul, the health system took a more focused approach. It began by identifying the vendor groups with the most frequent on-site presence and the greatest operational impact. This allowed leadership to concentrate on areas where improved oversight would deliver the most immediate value.

From there, the organization worked to define a practical baseline for these vendors. The intent was not to replicate clinical credentialing requirements, but to establish standards that reflected actual risk. Background screening, basic safety protocols, and clearer identification at the point of entry became the foundation.

Equally important was internal alignment. Facilities and support services teams—those interacting with these vendors on a daily basis—were involved early in the process. Their input ensured that the approach was not only effective on paper, but workable in practice.

Over time, the organization began to move toward a more consistent model, where service vendors were no longer treated as exceptions, but as part of a broader, unified credentialing strategy.

Conclusion

Vendor credentialing programs have long played a critical role in maintaining safety and compliance within hospitals. But the scope of that responsibility has expanded.

Hospitals are no longer managing a small, defined group of clinical vendors. They are managing a dynamic, distributed network of third-party individuals—many of whom operate outside traditional credentialing frameworks. Closing that gap requires updating the model to reflect how access actually occurs across the organization.

The systems that make this shift will be better positioned to manage risk in a way that is both practical and defensible. More importantly, they will gain something many organizations still lack: a clear, consistent understanding of who is on site and whether they meet the standards required to be there.