



Delivering Frictionless Security to the Clinical Workflow: Essential Requirements for Access Governance Solutions

A Frost & Sullivan White Paper

www.frost.com

Mike Jude, Ph.D.

Abstract..... 3

Introduction 3

Essential Requirements for Access Governance Solutions..... 4

Last Word 5

ABSTRACT

The clinical workflow defines the delivery of healthcare services to patients. As such, managing it efficiently is critical to achieving the Quadruple Aim of healthcare, as espoused by HIMSS: enhancing patient experience, improving population health, reducing costs, and improving the work life of healthcare providers, including clinicians and staff. Yet these objectives are hard to achieve when workflow automation is characterized by an expanding, complex ecosystem of devices, applications, and evolving delivery options. Complicating this is the increasing need for data security to ensure that only those clinicians who have the appropriate privileges will have access to sensitive patient data and IT systems. What is needed is frictionless security—security that is unobtrusive and comprehensive, and that doesn't hinder clinical workflows or the delivery of care to patients. Unfortunately, current security solutions, designed to address the needs of multiple industry verticals, fail to meet the specific needs of healthcare. An IT and security strategy driven by a holistic, integrated identity, governance, authorization, and access management solution purpose-built for healthcare is essential.

INTRODUCTION

Frost & Sullivan believes that a single-source, holistic access management approach is critical to a frictionless clinical security environment. However, while there are many security vendors—many of whom have excellent solutions—there are not many that provide purpose-built solutions for the healthcare environment.

Wading through the hyperbole and competing claims can be a daunting task for IT decision makers. Nevertheless, for the healthcare organization concerned with improving efficiency while containing or reducing cost, there is really no other choice but to devote resources to researching the options.

This paper provides a foundation for conducting that research. The essential requirements that one should look for in an access governance solution are provided with some explanation of the impact each has on the management of access across the clinical workflow. Only those solutions that can provide compelling evidence that they satisfy the full requirements should be considered.



ESSENTIAL REQUIREMENTS FOR ACCESS GOVERNANCE SOLUTIONS

The benefits of well-integrated access governance solutions are unassailable. The wonder is that so few healthcare organizations are pursuing such an approach. Frost & Sullivan believes that the problem is largely due to the complexity of existing healthcare informatics and confusion that exists in the minds of healthcare IT organizations when looking for such a solution.

While Frost & Sullivan cannot address the complexities of each individual IT implementation—especially since many can be considered to be custom—it can suggest a way to evaluate access governance solutions. In particular, decision makers should consider the following recommendations:

- **Select a single-access and identity management application suite:** Point solutions introduce overheads that rapidly erode both organizational efficiency and treatment efficacy. As noted previously, a single solution optimizes IT resources and facilitates a more efficient workflow. Additionally, such an approach enables much easier technology upgrades. IT technology is undergoing a major paradigm shift from data centricity to information centricity, but true information infrastructures will only surface when IT organizations are unburdened by routine access control activities.
- **Select single sign-on integration:** Reduce physician burnout by reducing the overhead of multiple sign-ons. As impactful as physician burnout can be, it actually comes with hidden impacts: burnout leads to degraded patient care and a general organizational malaise as the primary providers of quality healthcare begin to disengage emotionally from their responsibilities.
- **Focus on access management:** Single sign-on and authentication is important, but so are efficiency-promoting capabilities such as “tap and go” and location-sensitive access. Additionally, facilitating the efficient transfer of personnel into and out of the organization can save IT from routine access control activities.
- **Ensure the solution supports a rich and diverse ecosystem of access devices and work plans:** Access devices are proliferating. Existing mobile technology such as shared mobile devices and tablets are increasing the number of potential ways in which clinicians will access healthcare applications. In the future, new access modalities and devices will further complicate the access ecosystem. Security solutions will need to accommodate such new devices and the diverse work plans they support.
- **Look for out-of-box integration with EHRs, VPNs, and other clinical systems and applications:** Access management that requires customization to integrate with existing applications improves nothing and, in fact, only adds to overheads. Access management should be compatible with the most important applications out of the box. Moreover, the solution should offer tools to enable integration to other ancillary applications that may not offer API-level integration points or support federated authentication.
- **Select a solution that supports existing and evolving clinical workflows:** Clinical workflows are rapidly evolving to include such concepts as remote healthcare delivery and satellite clinical facilities. Providing identity and multifactor authentication for remote access is increasingly important to secure

such approaches. Additionally, DEA regulations, such as those for EPCS, mandate particular requirements for access to critical systems. Access governance needs to recognize all of these scenarios.

- **Look for a solution that includes identity governance:** Fast, secure, role-based access to EHR systems and applications is necessary to enable evolving, flexible clinical workflows. Implementing regular access certification and an attestation process ensures governance and compliance with corporate policies. Once again, overhead reduction is the criterion, and anything that helps minimize the loading on healthcare delivery is necessary.
- **Choose a solution that facilitates identity risk management:** Ideally, effective access governance should provide a comprehensive view of the security status of the organization. This should include a dashboard for the security and compliance teams to have a holistic view of potential risk areas due to over-assignments of entitlements.
- **Select a vendor that is able to articulate future enhancements:** A vendor that has no plans for future developments in access governance is unlikely to keep up with the rapid evolution of healthcare and will be unable to respond to developing requirements for patient security, cloud migration, and other new technologies and access methods.

Finally, it is important to look for a provider with successes to share—cutting edge, but well-tested and solid. The solution provider should provide references.

LAST WORD

Achieving a frictionless security infrastructure—one that does not impose needless overheads on personnel and that enhances workflow—is not easy when IT decision makers are unsure which security solutions can deliver such capabilities. Having a guide to solution selection simplifies the process by pointing out the essential properties that any solution must have.

However, making the right choice does not end with a simple review of sales literature. Any security solution provider must provide concrete examples of their capabilities so the decision makers can match those capabilities to the requirements. This can be time consuming but is critical to optimizing the security outcomes. The key objective is to select a security partner that can not only provide a plan for the present but also has a plan for the future.

Healthcare professionals, faced with securing an increasingly complex workflow automation environment, can't wait. The security landscape will only become more diverse and complex over time. It is important to select a vendor that can deliver a single identity and access governance solution that is capable of scaling as organizational needs change. Decision makers should consider Imprivata, a healthcare technology provider that is building such governance solutions today.





Silicon Valley
3211 Scott Blvd
Santa Clara, CA 95054
Tel +1 650.475.4500
Fax +1 650.475.1571

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel +1 210.348.1000
Fax +1 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost • myfrost@frost.com
<http://www.frost.com>

NEXT STEPS

-  **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
-  Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
-  Visit our **Transformational Health** web page.
-  Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
3211 Scott Blvd
Santa Clara CA, 95054