FROST & SULLIVAN

Delivering Frictionless Security to the Clinical Workflow:

The Need for a Healthcare-focused, Integrated Identity and Access Management Strategy

A Frost & Sullivan White Paper

www.frost.com

Mike Jude, Ph.D.

50 Years of Growth, Innovation and Leadership

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: COMPETING HEALTHCARE IT DEMANDS

Healthcare IT is focusing on how to ensure the security of the clinical workflow so that patient data is protected while necessary and authorized access to applications and systems is enabled. Complicating this requirement is the need to contain costs, a major concern as security increasingly consumes IT budgets. IT leadership is increasingly feeling the pinch of escalating demands for security on the one hand and more efficient operations on the other.

Yet not addressing this IT operations problem is not an option: the delivery of healthcare is increasingly dependent on technology. Healthcare delivery requires digital systems to manage such activities as admissions, clinical documentation, payment, treatment, and post-discharge monitoring. More applications are being delivered to more endpoint devices such as laptops, tablets, and smartphones. Additionally, the internet of things (IoT) is bringing a proliferation of new, connected medical devices. Technology is leading to increased complexity, both for IT as well as for clinicians, who must access critical applications to deliver healthcare services.

As complexity increases, the number of exploitable points of security vulnerability increases as well. This comes at a time when security is becoming a growing concern, not only for healthcare professionals but also for regulators and policymakers. The Health Insurance Portability and Accountability Act (HIPAA) is only one of many regulations governing the security of health information; now additional regulations governing the privacy of individuals, such as the EU's General Data Protection Regulation (GDPR), portend an even greater degree of sensitivity to the security of healthcare information. Nevertheless, even though security is critical, it can't be allowed to hinder clinical workflows or the delivery of health services to patients.

Satisfying these competing demands while ensuring application and system uptime is not easy, but making time to get ahead of this pernicious dynamic on a piecemeal basis can be virtually impossible. What is needed is a strategy for security, one that includes integrated, easier to support access management.

THE NEED FOR A HEALTHCARE-FOCUSED, INTEGRATED IDENTITY AND ACCESS MANAGEMENT STRATEGY

Clinical workflows are becoming highly digitized. In fact, contrary to common perception, healthcare was an early adopter of digital record keeping, as insurance carriers saw computerization as a key to managing the delivery of health services to millions of subscribers. Nevertheless, the utilization of IT in healthcare evolved as a series of discrete solutions, each of which was developed to address a particular need. Now, multiple applications define the workflow: admissions, treatment planning, computerized physician order entry, service delivery, and discharge. While each solution works well in isolation, they do not necessarily integrate well, which presents a problem when the objective is to deliver a seamless patient experience.

In particular, security, which should be managed as a common function across all stages of the clinical workflow, is by virtue of myriad applications, managed as a series of discrete touch points in the healthcare delivery process. Rather than providing a single point of access, modern healthcare IT frequently forces physicians and other healthcare providers to securely authenticate to access each of the many applications required during their day; most are accessed more than once during an average clinical work day.

HIMSS US Leadership and Workforce Survey identifies the concerns healthcare professionals have with modern automated workflows:

- Patient safety
- **Privacy, security and cybersecurity**
- Process improvement, workflow and change management
- Clinical information and clinician engagement and data analytics/clinical and business intelligence
- Improving quality outcomes through health IT
- Compliance, risk management and program integrity
- EHRs (impact on patient care)
- Consumer and patient engagement
- Culture of care and care coordination
- Leadership, governance and strategic planning

Exacerbating this situation is an expanding healthcare ecosystem that includes more mobile devices, more mobile physicians, a more differentiated ecosystem of access endpoints—virtual workstations and medical devices—and an increasing number of non-traditional healthcare delivery protocols. Clinicians, shifting from one treatment situation to another, may find that they must spend time logging in to applications they might have been using only a few minutes before, simply because they have moved to a different location or have shifted from a hospital ward to an on-premise clinic.

Yet the need for security demands that access to critical systems be controlled; each application requires access controls, some prescribed by law—electronic prescription for controlled substances (EPCS), for example. In this case, access governance is critical to the protection of patients, restriction of access to controlled substances, and the security of healthcare information, and the penalties for not doing so can be extreme. Even so, regulatory penalties can pale in comparison to the cost of losing data. Health IT Security News estimated that the average cost of a healthcare data breach in 2017 exceeded $3.62 million per instance, and the liability cost, which security breaches contribute to, can exceed 10% of the total cost of healthcare. In fact, the HIMSS US Leadership and Workforce Survey shows that privacy and security, including cybersecurity, are, collectively, the second most pressing concern of healthcare IT professionals. Of course, these costs ignore the unique nature of healthcare, where a situation which impacts patient outcomes may involve harm that cannot be undone.

Access management, then, is not an option; it is a necessity. However, inefficient and insufficient access control can lead to a breakdown in security. Forcing clinicians to repeatedly log in to locked applications and workstations tempts the use of shortcuts or bad security hygiene that increases the likelihood of stolen data. What is required is not only access control across the clinical workflow continuum, but access control that is seamlessly integrated into end-user workflows.

Access management should restrict access to critical applications and recognize access needs by individual and role. As a clinician is added to the workforce, effective access management will recognize the access profile that job position demands and enable it. When an individual leaves the organization, access must be rescinded.

Finally, access controls must be tightly integrated with existing health IT at a holistic level. Authentication methods that differ by application and endpoint will simply slow clinical workflows, aggravating healthcare providers and non-clinical end users. An access management solution that is purpose-built to address specific healthcare needs for speed, accuracy, and workflow optimization, is, therefore, a necessity.

Integrated identity and access management technology is part of an overall strategy of access governance, helping to manage which users are granted access to clinical systems based on their roles, while enhancing how end users authenticate into each system. Applied as a continuum across all clinical workflows, an access governance strategy should address the Quadruple Aim to not only improve healthcare, but also the work lives of healthcare professionals.

LAST WORD

Frictionless security, which is well-integrated into clinical workflows and provides the necessary access controls without too much overhead, is becoming increasingly important in healthcare. Yet frictionless security does not come without planning: a comprehensive access management strategy is required to ensure that security solutions support the entire clinical workflow continuum in a holistic, consistent way.

Adopting an access management strategy that improves efficiency, while standardizing access across applications, is the first step to controlling healthcare IT costs, as well as improving the productivity of clinicians and staff. Reducing the complexity of access is an important way to gain control over the complexity of the evolving healthcare delivery environment as well.

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.

FROST & SULLIVAN

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