FROST & SULLIVAN

Delivering Frictionless Security to the Clinical Workflow:

Access and Identity Management the Key to Workflow Efficiency

A Frost & Sullivan White Paper

www.frost.com

Mike Jude, Ph.D.

50 Years of Growth, Innovation and Leadership

TABLE OF CONTENTS

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

Having an access management strategy is critical to developing frictionless security in the clinical workflow. However, justifying this approach to a healthcare organization, where every technology investment is carefully scrutinized, depends on understanding the way in which access and identify management contribute to overall clinical workflow efficiency. Generally, this means ensuring that access and authentication do not impede the delivery of healthcare or overly burden clinical staff as they complete their tasks during each work shift.

In particular, with the increased focus on care coordination and the care team approach, patient information needs to be even more accessible. Healthcare providers need to ensure clinicians and staff have the right access for their job function, but not more than what is needed: this means adhering to the principle of least privilege, which limits access for those without a legitimate need or right and decreases the likelihood of data being improperly accessed, stolen, or misused. Such access management needs to account for clinicians moving from one job function to another, as well as the need to disable access when someone leaves the organization. This tension between the importance of protecting patient data and providing high-quality health services is leading to frustration between IT and clinicians.

Implementing solid access and authentication management solutions, which can provide the necessary and authorized access, can significantly reduce the overheads that security can impose on the clinical workflow. These can be as simple as reducing the overheads associated with sign-ons to as complex as reducing the impact on clinical efficiency that constant authentication can have. Additionally, the IT organization can be impacted by inefficient approaches to security that demand management of myriad discrete authentication processes.

Access and authentication, done right, can significantly improve clinical workflow and ensure a more comprehensive approach to security. Technology that supports single sign-on, in particular, can be the key to workflow efficiency.

ACCESS AND IDENTITY MANAGEMENT: KEY TO WORKFLOW EFFICIENCY

The aim of implementing security protocols is, at least in part, to ensure that the integrity of patient records is considered across the care continuum, shielding them from improper access and breaches in critical systems. However, the perception of security is that sometimes it can intrude on the appropriate delivery of healthcare services. The truth is that security can be either an enabler of clinical workflow efficiency or a significant impediment to the healthcare delivery process. Access and identity management, when done without a focus on process improvement, can impact clinicians and impose a significant overhead on IT support personnel tasked with granting and revoking access to health IT applications.

The typical IT organization can devote person-weeks to managing security, granting access to the various applications and systems that characterize key clinical workflows. The SANS Institute estimates that as much as 9% of the average enterprise-level IT budget was devoted to managing security in 2016. This is likely much higher now.

Complicating the delivery of healthcare IT is the task-sensitive nature of security. For example, depending on the task at hand, a clinician may use several different clinical systems. Each system may require a different level of access and each must be set by the IT organization. This can be further complicated when the security profile desired is only loosely specified by management. Simply stating that a new employee should be granted the same access as another employee can mean hours of research for IT, and even then, there is no guarantee that the access will be precisely the same, as employees change roles or tasks over time. Therefore, the access for this new user may end up being too broad than what they actually need, increasing the risk of unauthorized access.

Although the impact of access and identity management on IT can be severe, it can also impact the clinical staff that depends on the access that has been granted. According to a study conducted by Gellert et al. in 2017, physicians can spend up to 29.3 seconds per application sign-on selecting an application, providing a username and password, etc. While this might seem nominal, it actually has a profound impact on workflow efficiency in two ways.

First, such an interruption consumes time that incrementally adds up to significant levels over the course of a clinical work year. For a physician that routinely logs into an EHR system for each patient visit and who may have an average of 18 patients per workday, the number of sign-ons in a typical year can be as high as 4,320, based on a typical 240-day work year. This amounts to approximately 35 hours per physician per year or nearly a complete work week. Single sign-on (SSO), which reduces the number of discrete system and application authentications, could have a profound impact on this metric, effectively reducing the number of sign-ons from 4,320 to 240.

Second, an interruption that distracts a physician from providing care can introduce task-switching overheads that seriously degrade the level of care. It has been estimated by the American Psychological Association (APA) that, for technical work, switching tasks can consume anywhere from five to 30 minutes. While a person will not simply stop working while task switching, the APA estimates that such task switching significantly reduces cognitive efficiency. If the worker is a physician, task switching can impact the care a patient receives, as the physician is distracted from the primary function of providing care. For the same example above, a physician with 18 patients a day could expect anywhere from 360 to 2,160 hours of degraded performance over the course of a year, at a minimum nine weeks of degraded performance.

These examples, while staggering, do not begin to take into account all of the systems a physician might need to access. There are EHR systems, of course, but there are also countless other applications that are used in care delivery workflows. Each logon interrupts key workflows, breaks clinician concentration, and introduces task-switching inefficiencies.

Any workflow break adds to costs and diminishes the quality of patient care. Every point in the clinical workflow where providers must authenticate is another potential task interruption.

There is no question that security is increasingly important in healthcare:

- In 2015 alone, three large data breaches led to the theft of 95.5 million patient records.
- In 2017, the cost of data breaches exceeded $12 billion in the US healthcare market.
- In 2017, the total cost of data breaches exceeded $2 million per hospital.
- The average time to investigate and correct a security vulnerability was 55 days in 2017.

In aggregate, it is no wonder that physicians complain bitterly about the impact that health IT systems are having on patient care and their clinical work life. Yet access and identity management can also be a powerful force for improving workflow efficiency, especially if it enables SSO rather than incremental sign-ons to applications.

In particular, automated identity management and SSO can improve workflows by:

Reducing the number of sign-ons required: By enabling a single sign-on protocol, the number of sign-on activities and task interruptions can be radically reduced. This increases not only workflow efficiency but increases clinician satisfaction levels.

Providing an audit function: An increasingly important aspect of security and privacy management is ensuring that administrators know who is accessing which applications and when. Having an audit capability provides some certainty that patient data is being protected.

Reducing task-switching overhead: Security systems that enable single sign-on can significantly reduce the overhead associated with task switching. Rather than stopping and logging in to an application with each change of task or patient, the physician can log on once, saving the equivalent of person weeks of degraded performance over the course of a year.

Reducing physician burnout: Physicians who are forced to juggle too many administrative functions tend to burn out. Single sign-on that offloads the constant need to authenticate can substantially reduce one of the stressors that lead to burnout.

Enabling timely de-provisioning of all access when users leave the organization: One of the most significant threats to patient data is the loss of positive user control. This often happens when an individual leaves the organization and access to critical applications isn't rescinded. Access management that can recognize when an individual leaves and automatically de-provision access to such applications can substantially reduce the risk that employee departures pose.

Additionally, access management that is integrated into clinical workflows can also enable overhead-saving capabilities such as "tap and go" authentication—where a healthcare provider simply taps an access point with a security badge to gain access to appropriate and necessary applications and systems—and location-sensitive access. These capabilities are especially beneficial when a physician may be required to treat patients in a variety of settings or treatment venues.

Achieving these positive outcomes largely depends on how access management is applied to the clinical workflow. If the approach is to insert security at each point of clinical application access, then the result can be the kinds of overheads described above. However, if the approach is to integrate access control into the process—making security an umbrella function that a clinician interfaces with once in a duty cycle—then the result can be a measurable improvement in healthcare delivery efficiency.

LAST WORD

Access management is key to ensuring clinical workflow efficiency. Yet many healthcare providers are still approaching security using a piecemeal approach that treats each application and system as a discrete point of vulnerability that demands dedicated access control. Such an approach, while secure, imposes huge overheads on the clinicians, who are forced to authenticate to each system at each point in the clinical workflow, and also on IT, which must manage myriad security solutions.

A holistic view of security is necessary. Rather than inserting access control at every point of vulnerability or for every application, an approach which facilitates single sign-on across all of the applications and systems that a clinician might need is the only way to achieve real workflow efficiency. Ensuring that access and authentication are consistent across the many applications and systems necessary for managing the delivery of healthcare can save time and improve clinician efficiency. By reducing the amount of time spent signing on to applications and minimizing the interruption of the treatment process, access management can provide real, measurable benefits to the healthcare provider.

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