OPEN ACCESS Freely available online

ISSN: 2157-7560
Journal of
Vaccines & Vaccination

Case Study

Leveraging Identity and Access Management Technology to Accelerate Emergency COVID-19 Vaccine Delivery

George A Gellert*

Department of Health Informatics, CHRISTUS Health, San Antonio, Texas, United States of America

ABSTRACT

Background: COVID-19-related vaccine demand and delivery volume challenged delivery organizations as few crises have. Imperatives to ensure security of patient information, defend against cyber security threats, and accurately identify/authenticate clinician identity for patients remained. Creative deployment of Identity Access and Management (IAM) and Single Sign-On (SSO) to accelerate operationalization of a vaccine delivery center.

Methods and results: Innovative application of existing IAM/SSO technology implemented greatly accelerated vaccine delivery. Secure access enabled by IAM enabled a rapid expansion (25 minutes) for 500 new vaccine delivery personnel to be identified and authenticated during a pandemic peak.

Conclusion: Existing digital identity solutions enabled a vaccine delivery organization to accelerate secure identify management during COVID-19. Existing IAM investments and capabilities can greatly accelerate standing up emergent vaccine delivery capabilities and delivery sites within clinical service delivery and public health organizations.

Keywords: Vaccine; Clinical applications; COVID-19; Vaccine delivery; Hospital

BACKGROUND

Single sign-on and identity access management in routine hospital workflows

For many clinicians, Electronic Health Records (EHRs) have low usability and are regarded as a time consuming interruption to an already busy workflow, and to patient care [1-3]. The imperative to maintain the security of Protected Health Information (PHI) has historically involved password protection of EHR access, resulting in a need for clinicians to continually refresh complex passwords, which can impede clinical workflow. Hospitals have reported that clinicians typically login to 8-10 or more applications [4]. Entering, updating, and re-setting passwords uses time better spent on delivering patient care.

Single Sign-On (SSO) is a technology solution that eases and expedites clinician's access to the EHR and is a core platform in a hospital's Identity and Access Management (IAM) strategy and capabilities. SSO enables clinicians to login as usual by keyboard at the start of a clinical shift, and then streamlines all reconnect logins for the rest of the shift. SSO limits keyboard login to once a shift and accelerates access to clinical applications including the EHR and its PHI, eliminating the need for clinicians to create and remember complex passwords. Hospital objectives in implementing SSO is to provide clinicians expedited access to their clinical applications and the EHR, and to eliminate time expended in managing passwords. Once logged in at shift start, clinicians subsequently swipe a proximity identity badge on card readers sitting beside computer workstations. The proximity badge logs clinicians in and out as they roam the hospital/clinic. When the clinician moves to another workstation, the badge reader accesses the current state of the last computer used, automatically locking workstations when clinicians leave, and re-authenticating them upon return to where they last left off. SSO reduces repetitive, manual logins and expedites authenticated access to the EHR and clinical applications for the balance of

Correspondence to: George A Gellert, Department of Health Informatics, CHRISTUS Health, San Antonio, Texas, United States of America, E-mail: ggellert33@gmail.com

Received: 08-Feb-2023, Manuscript No. JVV-23-19844; **Editor assigned:** 10-Feb-2023, Pre QC No. JVV-23-19844 (PQ); **Reviewed:** 27-Feb-2023, QC No JVV-23-19844; **Revised:** 07-Mar-2023, Manuscript No. JVV-23-19844 (R); **Published:** 15-Mar-2023, DOI: 10.35248/2157-7560.23.14.511.

Citation: Gellert GA (2023) Leveraging Identity and Access Management Technology to Accelerate Emergency COVID-19 Vaccine Delivery. J Vaccines Vaccin. 14:511.

the clinical shift, after which keyboard login in the usual fashion is repeated to enable another shift of badge logins.

SSO provides support for varied applications used in clinics and hospitals. New applications can be profiled and deployed rapidly with SSO without coding. Password administration automates application password change processes, eliminating a burden for clinicians, who can focus on patient care rather than creating new passwords. By automatically launching/opening needed applications, time is liberated from computer keyboard for patient care. SSO implementation has been demonstrated to have a highly favorable impact with respect to clinician time liberated from keyboard/HER, and in net financial return on investment [5-7]. The introduction of SSO technology has been shown to facilitate adoption of key component functionalities of the EHR, including electronic clinical documentation, as well as related clinical applications [8-12].

IAM and an unprecedented urgency to scale population vaccine delivery during COVID-19

COVID-19 surges in patient volume disrupted the already complex digital identity and information environment of modern hospital/health system care delivery, and accelerated the adoption of telehealth/telemedicine. During the early phases of the pandemic, hospitals needed to ramp up clinical staff rapidly in order to manage an increased volume of very ill patients and patient triage. Clinicians and administrative staff had to significantly alter and adapt their workflows and worksites, and individuals not serving in direct clinical care roles worked remotely. All of the components of hospital COVID-19 response had to be completed while maintaining rapid, secure access to critical care delivery and operational applications and data. New, non-traditional treatment locations and centers in tents and mobile units, at hotels were established and had to use existing Information Technology (IT) infrastructure and capabilities to support both safe, effective patient care and information security and identity authentication. Vaccine delivery services were expanded dramatically, as well as improvised into new settings and environments to increase public outreach and access.

The pandemic and resulting patient volume surge crises amplified the importance and indeed the centrality of securing and managing digital identity across the healthcare delivery system in an emergent crisis, including implementation of mass vaccination efforts. Having core identity authentication and access management capabilities in place enabled hospitals and other care delivery organizations to leverage existing technologies in innovative ways to support and improve their COVID-19 institutional response effort, including those focused on secure identity and access management. Identity authentication and access management remained critical to securing the trusted digital identities of clinicians and patients during the pandemic, including many administrative and support service personnel whether on site in the care facility or working remotely and also facilitated effort to prevent hospital transmission of SARS-CoV-2 [13]. Table 1 presents a summary of eight use cases where hospitals and health systems deployed IAM to reduce viral spread in their facilities, to enable safer and low risk communications between infected patients and clinicians, and between patients and visiting family members (Table 1).

Table 1: Use Cases of IAM Technology Deployed in Hospital COVID-19 Response.

Use case value	Use case functional focus
Infection control and patient safety	SSO enabled clinicians to attest being symptom-free at shift start
Infection control and patient safety	SSO deployed for exposure and contact tracing of facility clinicians
Infection control and patient safety	SSO deployed to enable mandatory clinician temperature checks/reporting
Infection control, patient safety and PPE supply chain management	Inpatient telehealth consults and virtual inpatient rounding in isolation units to reduce infection risk and rate of PPE consumption
Infection control and patient/family well-being and psychosocial support	Mobile devices enabled virtual visits between isolated patients and families
Infection control and expedited authentication and workflows	SSO rapidly authenticated into mobile devices without touching screens
Infection control and maintenance of facility organizational effectiveness and work productivity	Secure access enabled for rapid expansion of personnel working remotely
Organizational staffing management, accountability and work productivity	SSO monitored attendance of temporary workers

This discussion will focus on a population health use of IAM technology to rapidly stand up a COVID-19 vaccine clinic in the United Kingdom. IAM enabled role-based access to rapidly on-board clinical care, vaccine delivery and support staff in the face of high patient volumes and vaccine demand, an imperative during the pandemic. This involved rapidly provisioning clinical application access to accommodate the substantial ramp up in staff needed to manage high patient volumes needing acute care, as well as populations requiring vaccination, and enabling access for expanded care and vaccine delivery staff.

METHODOLOGY

The National Health Service (NHS) in Northern Ireland–Health and Social Care (HSC)–is similar to the NHS in England, delivering care free of charge and providing social care services including home care services, family and children's services, day care services and social work services. The South Eastern HSC Trust is one of five Health and Social Care Trusts which provide healthcare, public health and social services

across Northern Ireland, including immunization services. The South Eastern Trust provides integrated health and social care services to multiple communities, serving a resident population of 354,651. In addition, acute care delivery at the Ulster Hospital serves a wider population.

In December 2021, in response to the highly transmissible SARS-CoV-2 Omicron variant, the Department of Health asked the Trust to set up a Regional COVID-19 Vaccination Center to facilitate the delivery and public uptake of COVID-19 booster vaccinations [14]. Due to the rapidly developing epidemiological and disease control situation, the new facility sought to be operational in five days.

In order to execute this mass vaccination initiative, additional staff were recruited and deployed, many of whom were retired nursing and medical staff, as well as nursing and medical students. Additional administrative staffs were also deployed to support the effort. Most of these new, temporary staff had no prior trust secure EHR, SSO and related information system IAM profiles, but nonetheless required immediate access to clinical information systems. Using the Trust's existing system for provisioning new user accounts would not have deployed rapidly enough, and manually would divert organizational focus and resources from critical areas such as the launching the vaccine center's operations in a timely manner.

Vaccine delivery organization setting

A newly and rapidly deployed Regional COVID-19 Vaccination Center in the South Eastern HSC Trust implemented to facilitate the delivery and public uptake of COVID-19 booster vaccinations. The Center would operate 12 hours per day, seven days per week, with a maximum capacity of delivering vaccinations up to 4000 individuals per day.

Operational challenge/imperative created by COVID-19

In establishing and rapidly stand up a new vaccine delivery facility in response to great need and demand during the COVID-19 pandemic, South Eastern HSC Trust faced a challenge of enabling rapid access to clinical systems for a new regional mass vaccination center, including the provisioning of vaccine provider secure identity access and authentication for 500 new temporary staff accounts. This required an agile identity governance solution in order to avoid a slow and labor-intensive manual process of staff onboarding and profiling. Concern existed that provisioning staff accounts could divert focus from launching other essential clinic operations. Equally critical, however, was enabling consistent access rights to all new, temporary users of the system Electronic Health Record (EHR), with rapid user onboarding, accurate authentication, and effective information governance and auditing capabilities.

Identity governance solution utilized

At the time, the Trust was already conducting a secure identity governance pilot of Imprivata Identity Governance which was focused on provisioning IAM to junior physicians, covering three cohort intakes per year. The pilot project involved setting up active directory and exchange accounts for new physicians who required access to 3-10 separate clinical systems, including PAS and the Ulster Labs application.

RESULTS

With the urgent requirement to institute a new vaccination center to drive community uptake and increase vaccination booster rates, the identity governance pilot project was rapidly pivoted to on-board up to 500 new clinical information user accounts. The identity governance solution was able to eliminate an onerous, time-consuming amount of inefficient manual work. The Center was able set up 500 staff accounts in just 25 minutes. The solution provided consistent access rights and authentication to all staff, based on their specific roles, and needed access to critical information systems.

When the vaccination center was decommissioned in late January 2022, staff accounts were decommissioned automatically, ensuring that sensitive, confidential patient data remained protected as accounts could not continue to be accessed. The solution also provided a clear audit trail of account provisioning and de-provisioning activity, which supported standards of effective information governance, security, and compliance.

Having proven the value of the identity governance solution, the Trust next sought to expand its use of the solution by adopting automatic triggering for junior physicians, so that as they move or alter their clinical roles and workflows, with changing secure information access and management needs, their permissions moved with them. It was also deployed manage the identity and information access needs of international nurses and domiciliary staff.

The identity governance solution has enabled NHS Trusts and other, diverse care delivery organizations to introduce precise role-based data access for all staff, thereby increasing the productivity of clinical staff by removing access barriers to technology. The solution strengthened data security with much accelerated cyber threat detection, evaluation, and remediation. Better managed regulatory compliance, with analysis of usage data *via* dashboards, was also achieved. Information technology costs were reduced by automating identity access and management. In addition, the solution provided a self-service portal for users to manage their own accounts.

DISCUSSION

In the midst of a public health and clinical care crisis such as a pandemic/outbreak of a highly transmissible pathogen like SARS-CoV-2, efforts to accelerate and reduce avoidable manual processes in establishing secure identity access and management at vaccination and clinical care delivery sites are essential. Identity management and governance solutions have a critical role in systematically compressing the time between the decision to institute a new vaccination site and delivery of the first injections into arms. In outbreaks of highly communicable pathogens, compression of the time required between policy and programmatic decisions to expand vaccine efforts and delivery of vaccine is a public health imperative.

In this case study, an identity governance solution enabled deployment of needed secure authentication and access provisioning to 500 vaccine delivery personnel with unprecedented rapidity and effectiveness. This analysis cannot quantify the burden of infection prevented in the South Eastern HSC Trust, or the resulting utilization in hospital emergency departments and ICUs avoided by greatly accelerating secure identity access/authentication and thus more rapid vaccine delivery. However, given the contagiousness of the Omicron variants of the virus during this period, these may have been substantial.

CONCLUSION

The imperatives to ensure the confidentiality of PHI and that only appropriate and authorized service providers and staff have access to critical clinical information systems are not diminished in a crisis, such as a pandemic. IAM systems are essential in enabling the right access of the right personnel to the right patient's clinical information at the right time.

Through most of the first three years of this pandemic, SARS-CoV-2 has demonstrated surprising and remarkable resilience and unexpected evolution. It is quite clear that, much as the last global pandemic of HIV/AIDS preceding it, COVID-19 will become a lasting focus within the healthcare landscape. The fact that less than two-thirds (62.8%) of humanity is fully vaccinated against the virus as of this writing implies that future variants of greater communicability and potential vaccine evasion are possible. Our healthcare system response and disease control/prevention efforts, including rapidly expanded and deployed vaccine delivery, require ever greater acceleration in pace of implementation. Given the case illustration and IAM/SSO technology solutions described here, future delays in enabling hundreds/thousands of care or vaccine delivery personnel to access critical information systems rapidly and securely during outbreak/pandemic response can and should be averted.

ACKNOWLEDGEMENTS

The author is grateful to the staff and leaders of the South Eastern Health and Social Care Trust in Northern Ireland for their public health service and embrace of technological innovation to improve COVID-19 response.

REFERENCES

1. Friedberg MW, Chen PG, Van Busum KR, Aunon F, Pham C, Caloyeras J, et al. Factors affecting physician professional satisfaction and their implications for patient care, health systems, and health policy. Rand Health Q. 2014;3(4):1.
2. Verdon DR. Physician outcry on EHR functionality, cost will shake the health information technology sector. Med Econ. 2014;91:18-20.
3. Hafner K. A busy doctor's right hand, ever ready to type. The New York Times. 2014.
4. Griffith A. Eliminate login nightmares with single sign-on technology. Health IT Outcomes. 2015.
5. Gellert G, Crouch JF, Gibson LA, Conklin GS. An evaluation of the clinical and financial value of work station single sign-on in 19 hospitals. Perspect Health Inf Manag. 2019;16(Summer).
6. Gellert GA, Delacerda C, Patel L, Maciaz G, Easing hospitalist EHR burden through clinical workstation single sign-on. J Hosp Adm. 2020;9:24-29.
7. Gellert GA, Ramirez R, Jacobs WJ, Maciaz G. Electronic Health Record Workstation Single Sign-on: A Quantification of Time Liberated for Nurses to Care for Patients. J Nurs Adm. 2020;50(9): 462-467.
8. Hope P, Zhang X. Examining user satisfaction with single sign-on and computer application roaming within emergency departments. Health Informatics J. 2015;21(2):107-119.
9. Fontaine J, Zheng K, Van De Ven C, Li H, Hiner J, Mitchell K, et al. Evaluation of a proximity card authentication system for health care settings. Int J Med Inform. 2016;92:1-7.
10. Laurello J. Challenges, Benefits of Implementing Single Sign-on in Hospitals. SearchHealthIT. 2013.
11. Hanover J. Best Practices: Single Sign-on Drives Productivity, Security and Adoption When Used with EHR at the Johns Hopkins Hospital. IDC Health Insights No. HI238582. 2012.
12. How single sign-on is changing healthcare: A study of IT practitioners in acute hospitals in the United States. Ponemon Institute. 2011.
13. Gellert GA, Kelly S, Hsiao AL, Herrick B, Lutz J, Weis D, et al. COVID-19 surge readiness: use cases demonstrating how hospitals leveraged digital identity access management for infection control and pandemic response. BMJ Health Care Inform.
14. World Health Organization. Coronavirus disease (COVID-19): Vaccines. 2022.