BMJ Health & Care Informatics

COVID-19 surge readiness: use cases demonstrating how hospitals leveraged digital identity access management for infection control and pandemic response

George A Gellert ,[1] Sean P Kelly,[2] Allen L Hsiao,[3] Brian Herrick,[4] Donna Weis,[5] Jeffrey Lutz,[6] Glynn Stanton,[7] Santos Bonilla,[7] Daniel Borgasano,[8] Matthew Erich,[8] Claire Reilly,[8] Daniel Johnston[9]

To cite: Gellert GA, Kelly SP, Hsiao AL, *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* 2022;**29**:e100680. doi:10.1136/bmjhci-2022-100680

Received 12 September 2022
Accepted 05 November 2022

Check for updates

© Author(s) (or their employer(s)) 2022. Re-use permitted under CC BY-NC. No commercial re-use. See rights and permissions. Published by BMJ.

For numbered affiliations see end of article.

Correspondence to
Dr George A Gellert;
ggellert33@gmail.com

ABSTRACT

Background Surging volumes of patients with COVID-19 and the high infectiousness of SARS-CoV-2 challenged hospital infection control/safety, staffing, care delivery and operations as few crises have. Imperatives to ensure security of patient information, defend against cybersecurity threats and accurately identify/authenticate patients and staff were undiminished, which fostered creative use cases where hospitals leveraged identity access and management (IAM) technologies to improve infection control and minimise disruption of clinical and administrative workflows.

Methods Working with a leading IAM solution provider, implementation personnel in the USA and UK identified all hospitals/health systems where an innovative use of IAM technology improved facility infection control and pandemic response management. Interviews/communications with hospital clinical informatics leaders collected information describing the use case deployed.

Results Eight innovative/valuable hospital use cases are described: symptom-free attestation by clinicians at shift start; detection of clinician exposure/contact tracing; reporting of clinician temperature checks; inpatient telehealth consults in isolation units; virtual visits between isolated patients and families; touchless single sign-on authentication; secure access enabled for rapid expansion of personnel working remotely; and monitoring of temporary worker attendance.

Discussion No systematic, comprehensive survey of all implemented IAM client sites was conducted, and other use cases may be undetected. A standardised reporting/information sharing vehicle is needed whereby IAM use cases aiding facility pandemic response and infection control can be disseminated.

Conclusions Clinical care, infection control and facility operations were improved using IAM solutions during COVID-19. Facility end-user innovation in how IAM solutions are deployed can improve infection control/patient safety, care delivery and clinical workflows during surges of epidemic infectious diseases.

WHAT IS ALREADY KNOWN ON THIS TOPIC

⇒ The innovative and adaptive deployment of identity access and management technology to improve hospital infection control and pandemic response has not been previously reported in the literature.

WHAT THIS STUDY ADDS

⇒ Eight use cases successfully deployed by hospitals in the USA and UK to improve SARS-CoV-2 facility infection control and pandemic response are reported.

HOW THIS STUDY MIGHT AFFECT RESEARCH, PRACTICE OR POLICY

⇒ With only two-thirds of humanity currently vaccinated against COVID-19, more virulent, contagious or vaccine-resistant variants of the virus may cause increased community transmission and future surges in patient volume, and these use cases can help hospitals improve their infection control and pandemic operations.

INTRODUCTION

COVID-19 disrupted the already complex digital identity and information environment of modern hospital care delivery and accelerated adoption of telehealth/telemedicine. Hospitals needed to ramp up clinical staff rapidly to manage an increased volume of very ill patients; clinicians and administrative staff had to significantly alter workflows and worksites; and individuals not serving in direct clinical care roles worked remotely, all while maintaining rapid, secure access to critical applications and data. New non-traditional treatment centres—in tents and mobile units, at hotels—were established and had to use existing information technology (IT) to support patient care and information security. Devices used to access information and communicate internally required rapid adaptation to reduce risk of viral transmission within the hospital. Use of mobile devices increased as iPads/tablets were used to support telehealth and facilitate virtual

BMJ Health Care Inform: first published as 10.1136/bmjhci-2022-100680 on 24 November 2022. Downloaded from http://informatics.bmj.com/ on February 6, 2023 by guest. Protected by copyright.

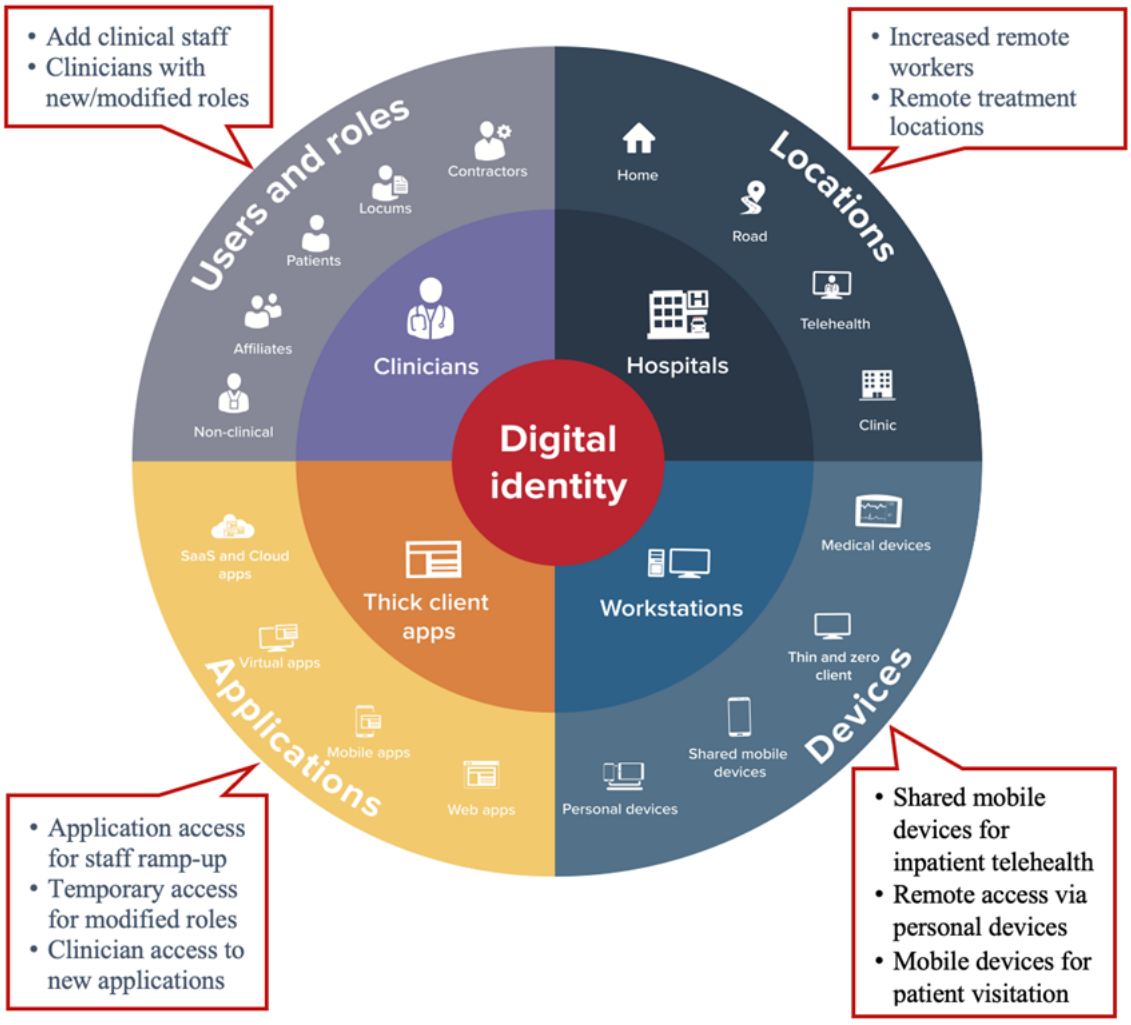

Figure 1 Hospital identity and information access challenges during COVID-19.

patient visits in hospitals, many requiring secure access management and a rethinking of existing high touch processes.

The pandemic surges amplified the centrality of securing and managing digital identity (figure 1). Identity access and management (IAM) capabilities enabled hospitals to leverage these technologies in innovative ways to support their COVID-19 response. A literature review found no use cases reporting IAM technology deployed to improve hospital infection control or outbreak management. Eight use cases are reported here which improved hospital operational and clinical response, reduced potential infection transmission within facilities and helped care providers and administrative staff, as well as patients and their families, cope with the challenges and risks created by the pandemic.

Single sign-on (SSO) expedites use of the electronic health record (EHR) by enabling a clinician to log in by keyboard only once at the start of a shift, and then use a proximity identity badge to reconnect for subsequent logins during the rest of the shift. SSO eliminates need to remember complex passwords, reduces repetitive manual logins and expedites authenticated access to the EHR and clinical software applications. SSO technology liberates substantial time from the keyboard for clinicians to focus on care delivery,[1–4] even more imperative during critical surges in patient volume. IAM remained critical to securing the trusted digital identities of clinicians and patients during the pandemic. Role-based access to quickly on-board clinical and support staff in the face of high patient volumes was imperative. This involved rapidly provisioning application access to accommodate the ramp-up in staff needed to manage high patient volumes and changing the access of certain clinical roles. Enabling access to shared mobile devices for clinician and patient use had to be accomplished securely, accurately and rapidly, as was secure access for a partially remote workforce.

The use cases were deployed to facilitate critical hospital operations during COVID-19 surges, and extend beyond the design intent of the solution vendor in three areas: (1) new workflows to monitor and mitigate risk of viral transmission and hospital-acquired infection within a facility; (2) inpatient telehealth care between care providers, and

BMJ Health Care Inform: first published as 10.1136/bmjhci-2022-100680 on 24 November 2022. Downloaded from http://informatics.bmj.com/ on February 6, 2023 by guest. Protected by copyright.

virtual visits of isolated patients with family members, to reduce risk of spreading infection within facilities; and (3) enabling IAM during rapid ramp-up of an expanded remote workforce. The technologies deployed in these use cases were Imprivata OneSign for SSO, Confirm ID for clinician identity and multifactor authentication and PatientSecure for patient identity validation.

METHODS

The reported use case data were gathered through communications between the customer support team of a leading IAM solution provider and health IT leaders among its hospital/health system customers. The particular IAM vendor was selected because of its high market penetration in the USA and UK, and because it was facilitating and recording which of its hospital customers were deploying its solutions in innovative ways to improve hospital infection control and COVID-19 operational response. Hospital/health system clinical informatics leaders were contacted in order to solicit a detailed description of how IAM and SSO technologies were leveraged to improve various clinical, infection control and/or operational workflows during the pandemic. Eight use cases deploying IAM technology to improve hospital/health system COVID-19 response were identified, all within the USA and the UK. These nations were a focus because they represent 80.2% (2320 US facilities) and 5.5% (158 UK facilities) of the IAM solution provider's total customer implementations worldwide.

Each use case was documented and shared with the involved hospital facilities in order to validate and improve the accuracy of its description. All recommended facility changes in descriptive use case content were incorporated, and the final report was shared with all hospitals/health systems for final review and approval. All hospitals/health systems known by the vendor to have deployed an innovative IAM use case during the pandemic and contacted in the development of this report also approved their identification, with the exception of one centre which was non-responsive and thus excluded.

RESULTS

Table 1 summarises the hospital facility value and functional focus of each of the eight use cases reported.

Table 1 Use cases of IAM technology deployed in hospital COVID-19 response by value and functional focus

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 organisational effectiveness and work productivity	Secure access enabled for rapid expansion of personnel working remotely
Organisational staffing management, accountability and work productivity	SSO monitored attendance of temporary workers

Key:
IAM, identity access and management; PPE, personal protective equipment; SSO, single sign-on.

SSO enabled clinicians to attest being symptom free at shift start

During an outbreak of a highly transmissible pathogen such as SARS-CoV-2, clinicians can inadvertently spread infection across the hospital. Having clinicians attest at the start of shifts that they were symptom free was critical to reducing viral spread. However, the symptom attestation process must be simple and rapid to ensure compliance and avoid disruption of clinical workflows and care delivery. To enable such rapid attestation and reduce the risk of clinicians adding to the facility burden of infection, hospitals needed a way for clinicians to log in and attest to 'absence of symptoms' with real-time reporting. Employees not providing care needed to be differentiated from those working in a clinical setting with elevated transmission risk to vulnerable patients and clinical colleagues.

A capability for attesting to the absence of COVID-19 symptoms was implemented which did not require all hospital staff but only clinicians at greatest risk of infection transmission to attest. Hospitals leveraged SSO to enable reporting of symptoms among only clinicians through a home-grown survey application that assessed for COVID-19 symptoms according to guidelines iterated by the US Centers for Disease Control and Prevention. This survey function was linked to SSO via an application programming interface so that when a user logged into a workstation, clinicians were automatically prompted to respond. There was no need to enter a username or password to log into symptom attestation, and multifactor authentication enabled users to quickly verify their identity easily and securely.

Hospitals implemented this functionality so it would not be intrusive and would only prompt clinicians once per 12-hour shift at shift start. Clinicians simply tapped their proximity card when prompted in the health attestation, confirmed they were symptom free, and could then begin work. Responses indicating a clinician could be positive for SARS-CoV-2 infection were automatically transmitted in real time to the hospital infection control team for review and appropriate response.

SSO deployed for exposure and contact tracing of facility clinicians

Yale New Haven Health, a system with seven hospital campuses, created a real-time process to monitor

BMJ Health Care Inform: first published as 10.1136/bmjhci-2022-100680 on 24 November 2022. Downloaded from http://informatics.bmj.com/ on February 6, 2023 by guest. Protected by copyright.

exposure and infection spread by using SSO workstation login records to help track and reduce risk of transmission from potentially exposed individuals. SSO reporting capabilities coupled with location logs enabled identification of exactly where and when users accessed specific workstations across all patient care areas, including those with infection risk. SSO audited the activity of clinical users when users authenticated to workstations, including user identity, workstation and date/time. Audit data retrieved from SSO cross-referenced with the known location of workstations (eg., Nurses Station 3 East) enabled granular infection contact tracing.

Combined with EHR data and workstation mapping, Yale first deployed SSO to accurately track infection exposure and transmission risk for measles and used the same approach to control facility spread of SARS-CoV-2. As clinicians are at risk of contracting infection when treating infected patients and may be exposed before patients exhibit symptoms, SSO detected if clinicians accessed a workstation near a patient or another clinician who subsequently tested positive. The real-time data generated by SSO enabled the facility to identify clinicians who had been in patient care areas where there was high potential risk of exposure and contracting infection.

Yale used multiple data points such as staffing lists to assess risk, while SSO conveyed granularity to identify specific users accessing workstations in units at elevated risk of infection exposure. With SSO providing the date and time of access, and how long it was used (duration of exposure), hospital infection control identified clinicians potentially at risk who accessed a workstation near a patient who was confirmed positive. This was accomplished by analysing data SSO collects when clinicians tap their proximity badge to access a workstation. By matching SSO audit data to location of workstation and patients confirmed positive, hospitals in future surges can determine which specific users were in areas with elevated risk of infection, for how long, and the infection control team can take necessary steps to interrupt further disease transmission. Leveraging SSO data in such a manner can be a powerful tool for infection control teams working to minimise pathogen spread during unexpected or novel outbreaks.

SSO deployed to enable mandatory clinician temperature checks/reporting

During COVID-19 surges, hospitals required clinicians to check and report their temperature twice per shift to monitor for potential infection. Hospitals and health systems with SSO, such as Yale New Haven Health, developed and deployed a home-grown internet-based application to support this workflow that was minimally disruptive for clinicians. Integrated with SSO, clinicians were able to badge tap into a workstation and access the application to report their temperature, ensuring the added workflow was fast and easy to complete. SSO also provided audit data to help hospitals track compliance with the twice per shift temperature reporting requirement. Here again, hospitals identified a use for SSO that was beyond its original design intent, but which delivered critical value in managing the crisis precipitated by COVID-19 volume surges.

Inpatient telehealth consults and virtual inpatient rounding in isolation units to reduce infection risk and consumption of personal protective equipment

During pandemic response, hospitals needed to minimise non-essential in-person interactions between care providers and infected patients to mitigate infection spread and to conserve limited supplies of personal protective equipment. Hospitals such as Nebraska Medicine, and in the UK the Royal Surrey NHS Foundation Trust, used iPads/mobile tablets or smartphones to facilitate on-site telehealth sessions with infected patients in isolation. Hospitals enabled clinicians to conduct clinical televisits without elevating clinician exposure/infection risk. Reducing contact with infected patients was critical to reducing viral exposure and transmission within care delivery settings. Royal Surrey used Ascom smartphones and the Attend Anywhere video consulting application for virtual rounds in the intensive care unit (ICU), with one physician rounding in person while linked remotely to colleagues.

To ensure patient confidentiality, a unique sign-on for each inpatient telehealth encounter was needed, and it was imperative to institute a hands-off login process. A comprehensive mobility solution (Imprivata GroundControl) was implemented at Nebraska Medicine to deliver automated provisioning, secure checkout and fast access to devices and applications. Clinicians tapped their proximity card on a docking station to check out a tablet for their shift. When accessing applications on the device, proxy credentials eliminated clinician need to manually type username/password. This enabled hospitals to automatically provision and digitally sanitise shared tablets, ensuring patient privacy through compliance with the Health Insurance Portability and Accountability Act (HIPAA), and helped hospitals set up, personalise and secure shared tablets. When finished, the device was returned to the docking station to be reset/cleaned and recharged for the next user.

Mobile devices enabled virtual visits between isolated patients and families

During COVID-19, hospitals instituted patient visitation restrictions to reduce risk of spreading infection. Patients—some at risk of death—were isolated from and unable to communicate with loved ones. Enabling virtual visits between isolated patients and family members on shared mobile devices was an important and humane part of care delivery during the COVID-19 crisis. A mobility solution for clinician telehealth encounters with isolated patients also enabled hospitals such as the University of Rochester Medical Center (URMC) to provide patients iPads/tablets for safe family visitation without sharing air space with infected patients.

BMJ Health Care Inform: first published as 10.1136/bmjhci-2022-100680 on 24 November 2022. Downloaded from http://informatics.bmj.com/ on February 6, 2023 by guest. Protected by copyright.

Mobile devices allowed quick and secure access to conferencing applications, enabling virtual inpatient family visits without risk of infection. Consumer chat applications such as Skype, Facebook Messenger and FaceTime were deployed with requisite privacy and information security measures. In providing iPads to patients for communication with visitors, URMC needed a way to provision, configure, wipe clean and reset devices back to a ready state for next patient use. In addition to physical disinfection, with SSO and a mobility solution it was possible to digitally sanitise identity on shared iPads/tablets while they were recharged to set up and secure the devices for use by other patients. In the UK, the Royal Surrey NHS Foundation Trust also provided virtual visits for patients in isolation, repurposing shared mobile devices accessed through SSO. A link sent to the patient's family connected to the virtual meeting with the patient, and at session end patient access was tapped out and the device cleared and cleaned for next patient use.

SSO rapidly authenticated into mobile devices without touching screens

During the pandemic inpatient nurses used mobile devices to share real-time patient vitals with remote physicians (e.g., in the ICU). Manual login while gloved is difficult and consumes time. Sharing mobile tablets increases risk of spreading infection, and during surges hospitals used SSO to enable staff to tap their badge to log in and out of devices during clinical care delivery. The Cambridge Health Alliance deployed SSO into their ICU Microsoft Surface Pro tablets to log in simply and rapidly and connect with remote physicians. SSO enabled badge tap in for instantaneous touchless access, mitigating infection risk and facilitating real-time communication with remote physicians.

Secure access enabled for rapid expansion of personnel working remotely

Patient volume surges increased the risk of hospital-acquired infection among attending clinical but also administrative personnel not involved in care delivery, and hospitals rapidly expanded the number of workers shifted to remote work. New York City Health+Hospitals (NYCH+H) sought to enable some clinical personnel, such as consultants, to work remotely when feasible. Remote workers needed network access that protected confidential patient medical information and secured against unauthorised access by cybercriminals taking advantage of COVID-19 to perpetrate phishing attacks.[2] Multifactor authentication was needed to help hospitals ensure information security as their remote workforce expanded. A solution providing fast, secure multifactor authentication for remote access, Imprivata Confirm ID, was provided to hospitals such as NYCH+H and Children's Hospital of the King's Daughters in Virginia. It enabled rapid expansion of secure access for remote workers with minimal disruption of critical workflows. Coventry and Warwickshire Partnership Trust in the UK was able to deliver secure home/remote work for more than 4000 staff from 60 different locations in several days.

SSO monitored attendance of temporary workers

COVID-19 surges forced many hospitals to rapidly ramp up temporary clinical and other staff. A challenge hospitals faced was a need to enable secure access and monitor staffing and work attendance of temporary workers to ensure appropriate staffing needs were met and to enable related financial processes. NYCH+H deployed SSO to enable temporary workers to badge log in at the beginning of shift, just as it does for permanent staff members. SSO authentication enabled hospitals to confirm when temporary workers had started their shift. This eliminated need for additional solutions to address this requirement, alleviating an operational concern during the pandemic when temporary workforces were alternately expanding rapidly and subsequently contracting as patient volume surged and waned.

DISCUSSION

A limitation of the methods used is the very high specificity but low sensitivity of vendor-identified use cases. We did not conduct a systematic survey of possible IAM-enabled COVID-19 response use cases among all customers of this leading IAM solution provider. Thus, it is possible that valuable use cases where hospitals deployed IAM technology to improve pandemic response and infection control were not known to the vendor among thousands of implemented facilities worldwide. Working with IAM solution vendors, researchers can establish a standardised use case surveillance and reporting process and vehicle where such valuable applications of IAM technology can be reported and detailed for sharing with the broader community of hospitals.

Hospitals may deploy these and other innovative applications of existing IT capabilities in future surges of highly communicable diseases, including and beyond COVID-19. Customisation of existing vendor technologies is often more easily and rapidly scalable—especially important during time-critical emergencies such as communicable disease outbreaks. Collaborative partnerships between hospitals and their IT vendors can help facilities implement such innovative solutions, whether in crisis response or routine operations. These use cases suggest hospitals and health IT vendors should regard solutions as an 'innovation sandbox' through which care delivery organisations can explore and innovate needed functionality, adding value and impact to existing products/services. In today's cost-conscious performance-focused healthcare environment—one likely to be challenged recurrently with future care crises—this may increasingly become imperative, not optional.

Hospital clinical, IT and administrative leaders should not regard the products/services they purchase from health IT vendors as static and delimited in terms of problems they can resolve and challenges vendors can help

BMJ Health Care Inform: first published as 10.1136/bmjhci-2022-100680 on 24 November 2022. Downloaded from http://informatics.bmj.com/ on February 6, 2023 by guest. Protected by copyright.

them meet. The necessity and urgency created by the pandemic crisis fuelled these hospital-inspired innovative applications of SSO and IAM technologies. However, patients, clinicians, administrators and payers alike will benefit when inventive and need-driven creative collaboration between hospitals and their IT vendors becomes the rule, rather than the exception.

CONCLUSIONS

Care delivery, patient-visitor and staff infection control and safety, and facility pandemic operations were improved by hospitals deploying existing IAM solutions creatively during COVID-19 surges. Facility end-user innovation in how IAM solutions are deployed, as driven by need, can reduce hospital spread of infectious pathogens and improve patient safety and care delivery by enabling more effective and safer clinical workflows during surges of highly contagious/epidemic infectious diseases. With only two-thirds of humanity vaccinated against SARS-COV-2, future variants of even greater communicability, virulence and potential vaccine evasion than we have witnessed thus far are possible.[5] Should substantial surges of patients requiring hospital care occur in coming years, facilities should consider whether these (and other) IAM use cases can improve their infection control capabilities and overall hospital COVID-19 response effectiveness.

Author affiliations
[1]Medical Advisor, Impact Demonstration, Imprivata, San Antonio, Texas, USA
[2]Department of Emergency Medicine, Harvard Medical School, Boston, Massachusetts, USA
[3]Department of Pediatric Emergency Medicine, Yale School of Medicine and Yale New Haven Health System, New Haven, Connecticut, USA
[4]Department of Health Informatics, Tufts University School of Medicine, Boston, Massachusetts, USA
[5]Department of Health Informatics, Nebraska Medicine, Omaha, Nebraska, USA
[6]Department of Health Informatics, New York City Health and Hospitals, New York, New York, USA
[7]Department of Health Informatics, Yale New Haven Health System, New Haven, Connecticut, USA
[8]Department of Clinical Operatons, Imprivata, Lexington, Massachusetts, USA
[9]Department of Clinical Operatons, Imprivata UK, Uxbridge, UK

Acknowledgements The authors are grateful to the clinicians who served selflessly during the pandemic, and to the hospital leadership teams whose innovations we have described.

Contributors All coauthors contributed either to the design or implementation of the innovative IAM use cases described, and/or the writing of the resulting manuscript. GAG is the author serving as guarantor.

Funding The authors have not declared a specific grant for this research from any funding agency in the public, commercial or not-for-profit sectors.

Competing interests GAG is an external medical advisor to Imprivata.

Patient consent for publication Not applicable.

Provenance and peer review Not commissioned; externally peer reviewed.

Data availability statement Data are available upon reasonable request. All data relevant to the study are included in the article or uploaded as supplementary information. All data relevant to the study are included in the article, in the form of output of communications and interviews with hospital personnel. However, no data set was generated for this study.

Open access This is an open access article distributed in accordance with the Creative Commons Attribution Non Commercial (CC BY-NC 4.0) license, which permits others to distribute, remix, adapt, build upon this work non-commercially, and license their derivative works on different terms, provided the original work is properly cited, appropriate credit is given, any changes made indicated, and the use is non-commercial. See: http://creativecommons.org/licenses/by-nc/4.0/.

ORCID iD
George A Gellert http://orcid.org/0000-0002-3519-7486

REFERENCES

1 Gellert GA, Crouch JF, Gibson LA, *et al*. An evaluation of the clinical and financial value of work station single sign-on in 19 hospitals. *Perspect Health Inf Manag* 2019;16:1.
2 Tidy J. How hackers are preying on fears of COVID-19. British Broadcasting Corporation news, March 13, 2020. Coronavirus: how hackers are preying on fears of Covid-19 BBC News; 2022 [Accessed 16 Oct 2022].
3 Griffith A. Eliminate login nightmares with single sign-on technology Health IT Outcomes; 2015.
4 Fontaine J, Zheng K, Van De Ven C, *et al*. Evaluation of a proximity card authentication system for health care settings. *Int J Med Inform* 2016;92:1–7.
5 World Health Organization, Our World in Data, Coronavirus (COVID-19) vaccinations. Coronavirus (COVID-19) Vaccinations - Our World in Data; 2022 [Accessed 16 Oct 2022].

BMJ Health Care Inform: first published as 10.1136/bmjhci-2022-100680 on 24 November 2022. Downloaded from http://informatics.bmj.com/ on February 6, 2023 by guest. Protected by copyright.