SailPoint

A Healthcare Case Study:

Identity Provisioning in the Face of a Pandemic

Globally, hospitals have faced an unprecedent public health event that has caused severe disruption to "business as usual." Modern health systems with previously tested crisis response and business continuity protocols in place have been challenged to ensure that information-related security and compliance are effectively maintained, even during a pandemic. In this case study, we showcase how one healthcare entity rose to the challenge.

The Challenge

This regional health system operates more than a dozen hospitals and specialized medical centers. It also provides management services to a handful of other hospitals. All told, the system has roughly 1,700 beds and more than 18,000 employees.

As a leading provider of general medical and surgical services, the health system maintains a disaster response plan with protocols for every department. The aim of the health system's plan is to create surge capacity for responding to a range of public health emergencies, from natural disasters to biological events to manmade crises such as terrorist attacks.

No amount of stress-testing could have prepared their plan for the current event, however, so hospital executives quickly discovered an important gap. Surge capacity involves freeing up hospital beds and securing additional medical equipment, but it can also require bringing on board hundreds of nurses, doctors and other medical personnel for the duration of the event. Some of them may work for other organizations. If the event were severe enough, the hospital might even have to call on retired specialists—cardiologists, intensivists, and pulmonologists—who hadn't pulled an emergency room or ICU shift in years.

The gap discovered by executives was the inability to accommodate a surge of requests from hundreds or even thousands of new users for access to the hospital's technology infrastructure. Like other hospital organizations of its size, the health system has a modestly staffed IT department. Provisioning new users—that is, setting up login credentials for the systems they need to access—typically took several days for the IT department to carry out. Anytime a healthcare professional is forced to wait for identity provisioning, lives can literally be put at risk. This risk was amplified in the current situation because normal options for routing patients to other providers were also disrupted. As with so many other parts of the healthcare ecosystem, previously accepted norms—in this case, identity provisioning for contingent workers—simply couldn't meet the demand caused by the surge.

Another Facet of the Challenge Emerges

To address this challenge, the health system had to reconcile an important tension. On one side was the imperative to onboard contingent workers in a rapid, seamless and accurate manner. On the other side was the obligation to maintain confidentiality, integrity and availability of protected health information (PHI) that flowed through the health system—e.g., applications and platforms.

The organization also faced a dilemma: Under previous disaster scenario testing, they had identified that key provider personnel may need to access hospital systems remotely. However, in the current situation, IT department personnel were also suddenly forced to work remotely under a pandemic quarantine because they were deemed to be non-essential personnel. This added another layer of complexity to ensuring that the right people had the right access necessary to do their jobs—quickly moving beyond scenario testing into a real-life scenario.

The Solution

For this health system, the way forward was to give users the ability to request system access on their own via SailPoint's Identity Security platform. SailPoint eliminated delays by automatically determining what applications and data each user could access, then providing the appropriate credentials for as long as the user had that role. Meanwhile, the platform's administrator dashboard offered a single, 360-degree view of access permissions for every user on every system across the enterprise. Built-in analytics allowed IT to run reports showing each individual's access history from the time of joining to the time of termination.

To solve the remote access issue, a SailPoint solution architect set up active directory groups to provide "bundles" of access over the internet. With this, the hospital could pivot to an emergency by making the Identity Security platform available on the internet temporarily. For example, a doctor working at a field hospital could gain access to the hospital virtual private network, email, electronic health records and a file storage drive all in a single request.

The access bundle feature makes it possible to securely and conveniently provision healthcare personnel and contingent workers on a very large scale. Suppose the health system brought in a thousand contingent workers. If those workers needed access to, on average, seven different applications in order to do their job, the platform could get hit with seven thousand access requests—one for each application. That number could go up exponentially if hundreds or even thousands of non-clinical employees were forced to work remotely. A bundle of access, defined in advance for each role, dramatically reduces the load, quickly gets workers up and running, and rapidly provides access to essential applications such as business productivity and collaboration tools.

The Takeaway

In a crisis or disaster scenario, many elements come together to enable patient care, not least of which is the ability to quickly assemble a large number of clinical and non-clinical personnel. However, ineffective or insufficient identity provisioning can create risks on several levels.

On the other hand, during a time of chaos an effective Identity Security platform can facilitate appropriate, policy-driven access rapidly, securely, and in compliance so that staff can carry out their work without delay. It can help reduce IT help-desk calls and free up IT resources for other critical activities even as it provides an encompassing, cross-organizational view of user access. Finally, it can provide a detailed audit trail so auditors can clearly see how the health system handled identity access during extraordinary times.

In a world where the unexpected can happen at any time, the ability to mobilize on a massive scale—while shielding sensitive data—is an essential competency no provider organization can afford to overlook.

Need to provision your remote workforce seamlessly and securely?

SailPoint Can Help.

ABOUT SAILPOINT

SailPoint is the leader in identity security for the cloud enterprise. We're committed to protecting businesses from the inherent risk that comes with providing technology access across today's diverse and remote workforce. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, and ensuring that each worker has the right access to do their job – no more, no less. With SailPoint as foundational to the security of their business, our customers can provision access with confidence, protect business assets at scale and ensure compliance with certainty.

PC1844-2104