3 KEYS TO MANAGING DYNAMIC WORKFORCE RISK IN HEALTHCARE
WHAT DRIVES HEALTHCARE WORKFORCE TRANSFORMATION

Today’s healthcare workforce is undergoing profound changes, sparked by digital transformation and the need to deliver better patient outcomes—and the fact that the internet of medical things (IoMT) is continually evolving how we connect to information and to each other.

Patient Wellness

In an attempt to better manage healthcare costs, many large employers are encouraging employees to take wellness into their own hands, with programs, apps and information that let people monitor and control their own healthcare decisions. Smart medical devices including wearables, mobile apps, sensors and monitors are becoming more and more widely used, giving patients access to their own information and personalized attention around the clock. In this landscape, healthcare professionals, patients, and third parties need secure, rapid access to information via mobile and web-based applications and data (including electronic protected health information [ePHI]) stored across interconnected and online systems.

Digital Transformation and IoMT

Digital technology improves patient care, while offering healthcare facilities and providers more convenient options for how and where they provide it. For example, telemedicine makes it easier for providers to provide care remotely and from multiple facilities, even for patients in remote locations.

Local Delivery Models

Healthcare workers who serve patients in multiple locations need to be able to access data on their devices as they travel, work from home, visit patients or work across healthcare facilities.
As healthcare organizations continue to work toward delivering better patient outcomes, they must adjust to these new workforce dynamics—but they also face a number of new threats.

An Expansive Ecosystem
The healthcare ecosystem is complex and includes many contributors to patient care and delivery, including large and small medical practices, hospitals, clinics, public and private payers, research institutions, pharmacies, labs, device manufacturers, and a myriad of healthcare providers. While the shift to a dynamic, mobile healthcare workforce has many advantages, it exposes organizations to the risk of improper user access to protected health information (PHI) and other sensitive information because of the vast array of devices used across the IoMT. It also becomes more difficult to effectively monitor the online activities of business associates, third parties, “gig” or contract workers, and others accessing a growing pool of shared data from often unsecured apps, connected devices (including wearables and monitors) and electronic medical records (EMRs).

A Revolving Door
Healthcare organizations are increasingly turning to business partners and contract staff to provide hard-to-find skills as a result of implementing new technologies, or because of physician and medical specialist shortages. Bringing on such external workers creates a revolving door of “joiners, movers and leavers,” along with unvetted personal devices that can be hard for IT departments to manage. If access isn’t managed diligently throughout the engagement lifecycle, security could be compromised—leading to cyber attacks, loss of patient data, impacts on reputation and compliance violations.

Privacy Concerns
With patients and providers generating a constant flow of interconnected patient information, patient data privacy becomes a central issue. The availability of real-time data and advanced analytics can generate insights that drive health and well-being—but organizations must not compromise security and patient privacy in the process.
How do these workforce risks materialize across your organization? In a recent survey, respondents admitted to engaging in at least one of the following unsafe behaviors at work¹:

- 46% using public (unsecured) Wi-Fi to connect to company resources
- 49% sharing confidential data via personal email accounts
- 17% losing devices, such as laptops and phones, with company information on them

Perhaps even more telling, nearly one in four respondents said they engaged in unsafe behavior simply to get their jobs done, while 18 percent revealed they didn’t know their actions were risky. Although cybersecurity training is extremely important to any digital risk management program, organizations cannot rely on workers to always do what is in the best interest of the organization.
The dynamic healthcare workforce is an important factor in providing the care that patients are demanding, but it comes with increasingly complex cybersecurity and risk management challenges. The more people accessing your systems, the more identities you must manage—and the greater the odds that one or more will be abused or compromised, potentially leading to a security breach or data privacy violation.

To manage dynamic workforce risk, you need three capabilities:

**Identity assurance:**
Verify that users—and entities—are who they claim to be, with easy, risk-based authentication that works across multiple platforms and environments.

**Access assurance:**
Get a complete picture of the resources each user can access. Understand what users can do in each access scenario—for example, who can access PHI and other intellectual property—and how related access risks could affect security and your compliance posture.

**Activity assurance:**
Get insight into what users do after they’ve logged into resources. This will help you identify who is accessing PHI, inappropriate activity and increase your chance of spotting compromised credentials and insider threats.
Identity assurance, access assurance and activity assurance. With these capabilities in place, you’ll be able to answer these key questions—indicating that your healthcare organization is well on its way to managing dynamic workforce risk.

**CAN YOU ANSWER THESE CRITICAL QUESTIONS?**

- **How do you know users (or entities) are who they claim to be?**
- **Do users have required access rights, and are these rights appropriate for their roles?**
- **Can you prove what a user or entity does and doesn’t have access to?**
- **Are you keeping workers agile while still protecting resources?**
- **How will you respond to intentional and unintentional access abuse?**
How RSA Can Help

Understand and assess your organization’s ability to deal with cyber threats to your healthcare systems and patient data.

Improve your ability to detect and respond to cyber threats quickly and efficiently across your systems.

Reduce your risk of external attacks and insider threats with modern, mobile multi-factor authentication; real-time detection of suspicious access and entitlements; and automated, risk-based identity governance controls.

Detect and respond to fraud threats in your patient-facing digital channels with a combination of actionable fraud intelligence, real-time behavioral analytics and risk-based adaptive authentication.

Provide organizational context and coordinate the response and minimize the impact of security incidents to your healthcare organization.

See more resources that can help you take the next steps toward managing dynamic workforce risks: RSA—Manage Dynamic Workforce Risk.
DIGITAL RISK IS EVERYONE’S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

1 Dell End-User Security Survey, 2017