RES

NO GOOD CHOICES?

WHAT TO DO WHEN PATIENT CARE AND IT SECURITY COLLIDE

A RES point of view on resolving the most vexing challenge facing healthcare IT leadership

Tuesday, 10.20 a.m.

A large suburban hospital's oncology ward

Will Rand, already halfway through his planned 30-day visit, clicked on an icon for a patient's radiology image. "Not authorized for this application," the screen displayed. Even with an anxious patient looking over his shoulder, Rand couldn't resist a moment's venting. He slammed the heel of his hand onto the keyboard and said, "Sorry, but they don't realize how much time this takes. This must happen 40 times every day." He sighed heavily and began tapping on the keyboard.

Friday, 08.40 a.m.

An outpatient center's admitting office

Jamie Grier was aware of her patient's growing irritation as she clicked through record after record. She had a stack of papers her patient had signed — records release, HiPAA, medical history — and they all had to be scanned, uploaded and sorted. She was having more trouble than usual. Her IT contact had said something about "profile corruption," whatever that meant. But whatever it was had cost her two days' of productivity in the past two weeks. There must be a better way. Her patients were suffering, sometimes literally.

Healthcare organizations exist to prevent health losses, to preserve health, or to restore health to the greatest degree possible. Therefore, delivering quality patient care is the primary concern of every healthcare professional. And that concern can be traced through the ranks from executive tiers to entry-level workers, and laterally across every part of the organization. In theory, this means that every other objective of the organization and its professionals should be compromised — to the lowest extent possible, but compromised nonetheless — in the pursuit of better quality patient care.

Either edge of the blade is more than capable of causing staggering harm to the organization in terms of data losses, liability losses, hard costs and the destructive effects of an injured reputation.

THE DOUBLE-EDGED SWORD OF SECURITY AND COMPLIANCE.

While this is easily said, it's not so easily done. Healthcare organizations are not just patient care centers, they are vast warehouses of highly sensitive patient data: personal contact details, personal identification numbers, insurance data, medical histories, credit card and bank account information, and much more. They also maintain this information for the most vulnerable members of society, including children – people for whom data breaches can endure for many years without discovery (a reality well known to those who exploit such data).

Governments have developed vast libraries of regulations driven by the need to ensure that the protection of this sensitive data is mandatory. While such regulatory actions are taken with the best interests of the patients in mind, over the passage of time compliance burdens have steadily mounted (old regulations are rarely retired, but the pace of creating new ones seem to accelerate).

It's a double-edged sword indeed, and either edge of the blade is more than capable of causing staggering harm to the organization in terms of data losses, liability losses, hard costs and the destructive effects of an injured reputation.

As the organizational arm charged with both protecting the warehouse of data and the systems that house it, as well as being an instrument of regulatory compliance, IT professionals are in a precarious spot. And they haven't wasted any time. Layer upon layer of security measures are in place to protect data, to mitigate against potential losses, and to enable the necessary compliance actions and reporting.

- Firewall security
- Anti-virus scans
- Data and system encryption capabilities
- Risk management and detection
- Endless amounts of compliance and information privacy training sessions

Every one of these actions — and likely many others in your organization — must be accomplished. With draconian consequences for healthcare organizations that do not comply, there are no options. IT must secure the environment, and — as layers of security and compliance measures are put in place — doing so will certainly have a negative impact on the productivity of clinicians.

Every organization is faced with this conflict, but the price for healthcare IT is much higher: it translates directly into reduced quality patient care. With the goal of better patient care paramount, what can IT do to remove barriers to clinician productivity without sacrificing security and compliance?

NO GOOD CHOICES — BUT COUNTLESS REASONS TO ACT.

Data breaches and cyberattacks are serious concerns particularly among healthcare organizations. A recent study by the Ponemon Institute found that healthcare organizations incur the highest costs for data breaches compared to any other industry. In the US, the cost of a healthcare organization's data breach was $398 per record compared to the mean average of $217 across industries.

In the US, the cost of a healthcare organization's data breach was $398 per record compared to the mean average of $217 across industries.

Growth pressure is sweeping the industry and many healthcare organizations are subject to consolidation. That's why a PricewaterhouseCoopers report described 2016 as the "year of merger mania." If achieving growth targets sustainably is the greater priority for your healthcare organization, then you need to focus on streamlining the digital workspace to improve productivity for both clinicians and IT.

You do have choices — good ones — that you can put into effect right away. Depending on whether you need risk reduction or productivity improvements, your next step in the evolution of the digital workspace can productively focus on the following five priorities.

REDUCING RISK

At a glance

- A strong safety net around the digital workspace can mitigate the risks of human error, and thwart cyberattacks

A recent two-year study found that healthcare providers and medical device manufacturers have a blind spot when it comes to cybersecurity: they focus on protecting patient data while largely ignoring increasingly sophisticated threats to patient healthcare itself.

Cyberattacks are increasingly the work of organized crime, terror groups and foreign governments. This new generation of cybercrooks is launching sophisticated ransomware attacks that lock out clinician access to vital medical apps and systems, putting patient health in immediate jeopardy. And they're raising the game. The latest ransomware trend, called doxware, combines the concept of ransom with blackmail, raising the stakes further and making the "old fashioned" FBI warning screen seem tame by comparison.

This is why leading healthcare IT teams are building safety measures directly into the clinician's digital workspace. Designed to thwart phishing attempts and prevent clinicians from accidentally launching malware, these measures include:

- Application whitelisting and read-only blanketing: Restricting clinicians to run only authorized applications based on their roles and applicable security policies, so accidental clicks cannot execute malware or unauthorized applications. With read-only blanketing, clinicians can only read files and data on the healthcare network and not update them unless specifically authorized to do so.

- Dynamic access and digital endpoint controls: Limiting each clinician's level of application and system access based on their profile and tasks so hackers can't take advantage of unrestricted access controls. Securing all digital entry points into healthcare networks including connected medical devices as well as USB and other portable drive ports, so malware cannot gain a foothold into the network and the critical medical equipment it supports.

MORE EFFICIENCY & PRODUCTIVITY

At a glance

- Automating routine tasks and providing clinicians with self service to reduce cost and deliver innovations, and improve IT agility to quickly adapt to emerging trends

Healthcare IT can no longer afford to be bogged down helping clinicians reset passwords, update profiles or access printers. These and other routine, manual requests are the low hanging fruit that are ripe for automation — which frees up IT for more value-added activities. And today's healthcare organizations need IT to evolve into a stronger, more strategic partner that will provide the services and agility necessary to help the entire organization navigate an uncertain future.

Mergers and acquisitions are a major trend among healthcare organizations. Whether acquiring a healthcare organization or being acquired by one, IT can automate many of the critical tasks necessary to bring the two organizations together. And regardless of the specific needs of your organization, your IT team can seize automation opportunities across the digital workspace by:

- Automating manual IT tasks such as user account provisioning, server and application lifecycle management, and application and service delivery
- Expanding the integration and access of different systems across your network with EMR and user account integration, application layering, and delegated access

FAST, SEAMLESS ONBOARDING AND OFFBOARDING

At a glance

- Centrally manage the entire identity lifecycle of each clinician so that any change in clinician status is instantly propagated across all systems

For many healthcare organizations, constant changes in the workforce are par for the course. In teaching hospitals for instance, visiting clinicians come and go and clinician roles change often. And the process of getting clinicians fully on board with the applications, services and data they need is highly manual and time consuming. In fact, it can be equally time consuming to disconnect clinicians from those same resources or make changes as existing clinicians assume new roles.

IT can take advantage of integration and automation opportunities to make workforce changes seamless and instantaneous.

With clinician productivity and information security hanging in the balance, IT can take advantage of integration and automation opportunities to make workforce changes seamless and instantaneous. And reducing manual steps almost by definition yield improved governance and security. You can centrally manage the entire identity lifecycle of each clinician so that any change in clinician status is instantly propagated across all systems — from HR and payroll to EMR and diagnostic applications. This makes it possible for managers to update the status of their clinicians without IT involvement, and to do it securely and accurately so that all audit and compliance requirements are met.

PERSONAL SELF SERVICE FOR CLINICIANS

At a glance

- Securely automate the delivery, access and removal of applications and services based on personally-initiated requests aligned with workflow and manager approvals

Your clinicians are just like any other consumer: they want everything to be fast and convenient, they want to do as much as possible from a mobile device, and they don't want to call your service desk. Ever. But the power of automation in healthcare can free clinicians to be more productive. When IT can securely automate the delivery, access, and removal of applications and services based on security policies and manager approvals, clinicians save time in getting what they need, such as resetting their own passwords or ordering equipment without intervention.

And to truly deliver next-generation self service to clinicians, IT must make those services policy-based and robust enough to meet the clinician's unique needs. For example, a clinician should be able to order a specific brand of headset and dictation software that only she needs, or request access to an obscure medical research library without hassles. And IT can go further by delegating access to products, applications, and services to approved roles, so managers can fulfill requests on behalf of clinicians wherever it makes sense.

GOVERN CLINICIAN USAGE

At a glance

- Improve usage visibility across applications, systems and services to reduce audit and compliance costs and optimize spending on software.

The risks to healthcare organizations include compliance risks such as violations of technology vendor license agreements and unauthorized access to confidential patient information. In fact, HIPAA audits are on the rise following a string of enforcement actions against healthcare organizations across the US. And in Europe, a brand new regime of stricter data protection rules coupled with aggressive penalties will be adopted across the EU by April 2018.

Healthcare organizations must gain detailed visibility into who is accessing what applications and services. This allows healthcare IT teams to reduce the time and effort required to meet audit requests from vendors, while avoiding significant penalties from regulators. Better usage visibility across applications, systems and services reduces audit and compliance costs and optimizes software spending. With application usage monitoring, for example, you may discover that only a third of your physicians actually use expensive 3D imaging software. That information can help you reduce licensing costs.

With advanced management software that forms the heartbeat of the clinical digital workspace, very significant benefits are well within your reach.

YES, THERE ARE GOOD CHOICES.

They can be surprisingly simple and quick to implement, focusing in many cases on tools that can turn manual, repetitive tasks into quick and efficient automation. With advanced management software that forms the heartbeat of the clinical digital workspace, very significant benefits are well within your reach.

- **Exceptional end user experiences** — keeping your clinicians and any information they need instantly accessible and secure, no matter where or how they are working.
- **People-centric security** — adapting applications and services based on each clinician's specific role, authorizations, personal preferences, and location.
- **Automation** — eliminating manual, inefficient IT tasks to make the delivery of your applications and services a standardized and seamless experience.
- **Self service** — giving clinicians on-demand access to the apps and services they need, including unique, one-off requests.
- **Predictability** — speeding clinician access and set up of applications and services with secure and pre-defined workflows that are consistent and standardized with applicable policies and approvals.

To learn more about these and other capabilities that will equip you to create, automate and secure the digital workspace, contact RES at www.RES.com.

ABOUT RES

RES creates, automates and secures digital workspaces to improve the experience and productivity of the workforce while lowering IT costs. RES takes a people-centric approach to making technology access secure, even in complex multi-device/multi-location scenarios, across physical, virtual and cloud environments. RES boasts numerous patented technologies, fast time to value, and superior customer support for more than 2,500 companies around the world. For more information, visit www.res.com, contact your preferred RES partner, or follow updates on Twitter @ressoftware.