CITRIX®

Innovations for Security and Compliance in Healthcare

Empower healthcare professionals while addressing challenges related to regulatory compliance, and cyber threats.

The latest healthcare IT innovations not only help clinicians deliver care more effectively, in more places—they can also support improved security, privacy and regulatory compliance. The experiences of three leading healthcare organizations show the transformative impact of Citrix solutions for healthcare IT.

This white paper explores technologies that enable organizations to maintain security, privacy and compliance while evolving their IT environment to increase clinician mobility and optimize patient outcomes. Citrix solutions for healthcare help customers transform the clinician and patient experience and accelerate organizational change while safeguarding electronic protected health information (ePHI) and other sensitive data, as illustrated by the experiences of Southcoast Health System, Franciscan Missionaries of Our Lady Health System and Nicklaus Children's Hospital.

Healthcare organizations face new challenges as they seek to embrace innovative and mobile models for the delivery of care. At the same time, this more dispersed information environment complicates security and compliance with regulations and standards such as HIPAA/HITECH, PCI DSS and The Joint Commission. Moreover, there is an increasing risk of cyber threats such as ransomware, especially due to vulnerabilities in legacy systems. More than ever, healthcare organizations need a comprehensive strategy to maintain security, privacy and compliance wherever they deliver care. Virtualization, mobility, and EFSS (Enterprise File Synchronization and Sharing) make it possible for care providers to access patient data and clinical systems more easily, more securely and in more places, ultimately resulting in better patient outcomes.

The opportunity—empowering clinician mobility

Mobility can play a vital role in helping healthcare organizations support clinicians, deliver care and optimize patient outcomes. Electronic medical records (EMRs) make patient data, test data, medical images, video and other information securely available wherever care is delivered. Empowered with digital workspace technology, doctors and nurses can access clinical systems and apps from anywhere, and choose the right device for any scenario—including their own, under a secure bring-your-own-device (BYOD) policy—from a PC in a practice office, to a laptop at home, to a tablet on rounds. With session roaming clinicians are mobile. The current state of their desktop, apps and files is just a few seconds away on any device as they move from office to prep room to exam room and other locations.

The benefits offered by these capabilities are clear and compelling. Healthcare organizations can:

- Optimize their delivery of care by improving clinician productivity and quality of patient interactions through fast, seamless follow-me access to clinical systems and information across any device and location. Practitioners spend less time logging in to systems, waiting for applications to launch and drilling into patient context so they can focus on their patients instead.
- Improve satisfaction and work-life balance for clinicians through increased flexibility and convenience, such as the ability to do much of their administrative work at home instead of having to spend additional time at the office, clinic or hospital.
- Increase operational efficiency by enabling doctors and administrators to get more done in more ways, more quickly.
- Empower collaborative, seamless, patient-centered care by helping distributed clinicians connect and collaborate securely across practices, hospitals, clinics, long-term care facilities, and other entities and locations.

Security, privacy and compliance challenges in next-generation healthcare IT environments

The transformation of healthcare through mobility is already well underway—but as they work to realize its benefits, organizations must also grapple with significant challenges related to security, privacy and regulatory compliance. Already difficult enough in a traditional IT environment, these issues become still more complex as clinicians, administrators and patients access applications and data in more ways, in more places, on more types of devices. In this increasingly mobile and diverse environment, IT must find effective ways to ensure compliance with standards such as Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and EMR incentive programs; deter cybercrime, such as ransomware attacks; and address non-malicious system vulnerabilities before they can expose the organization to risk.

The multimillion-dollar impact of HIPAA violations

HIPAA and the related Health Information Technology for Economic and Clinical Health Act (HITECH) introduced stricter rules around reporting data breaches and other incidents. This is understandable and necessary given the rising prevalence of incidents in the industry. The cause for these incidents can range from hacking, phishing attacks or theft, to inadvertent data loss, to bad organizational account management practices; whatever their origins, the ramifications for patients can be severe. While customers whose credit card data has been stolen can simply change their account numbers, a patient whose personal health data has been compromised may have to live with this violation for a long time.

For organizations that commit a second violation of HIPAA within the same year, fines have now increased six-fold from $250,000 to $1.5 million. These federal penalties are only the beginning; additional costs include investigations, legal fees, system downtime, lost credibility and lost business. These incidents pose a risk not just to the organization's bottom line, but to the liberty of its employees as well. As a federal law, offenses under HIPAA can be tried in federal court, and those who lose or misuse patient data can face prosecution for a class 3, 4, 5 or 6 felony depending on the nature of the incident. In the words of one Citrix customer, "If you lose personal data, you punish yourself. If you lose corporate data or intellectual property, your company punishes you. If you lose patient data, the law punishes you." Considering that a majority of healthcare organizations have committed more than five violations, the seriousness of the situation is clear.

PCI DSS—the overlooked mandate

Beyond HIPAA, healthcare organizations must also maintain compliance with PCI DSS by safeguarding patient payment card data and ensuring that their network environment provides protection against malware and unauthorized connections. While PCI DSS receives much attention in the financial and retail industries, where payment cards are central to business models, many healthcare organizations have been slower to recognize and address their own obligations under the standard. In some cases, this may result from the belief that Medicare reimbursement is not contingent on PCI DSS compliance. In reality, any organization that accepts a credit card is considered a "merchant" by the payment card industry, regardless of whether account numbers are stored, and is subject to its standards. Indeed, this compliance is part of the contract that merchants must sign with any card brand, and the PCI can penalize noncompliance with fines, fees and other costs.

Another reason that many healthcare organizations may avoid dealing with PCI DSS is the sheer complexity of its requirements, which include hundreds of specific and detailed measures covering security management, policies, procedures, network architecture and software design. Even for organizations that recognize the importance of PCI DSS, it may be seen as a lower priority than HIPAA/HITECH compliance or new investments in innovation, not to mention the extensive resources required to maintain existing systems. As a result, many healthcare organizations are only an audit away from being found in violation of PCI DSS—and liable for the resulting penalties and costs.

Further related challenges

The list of security and compliance challenges facing healthcare IT departments extends well beyond HIPAA and PCI DSS. To name only a few examples: The Joint Commission (TJC), formerly known as Joint Commission on Accreditation of Healthcare Organizations (JCAHO), poses accreditation requirements necessary in most states for licensing and Medicaid reimbursement. To earn the financial incentives available through Medicare and Medicaid for the "meaningful use" of certified EMR technology, organizations must meet thresholds for recording patient information as structured data, exchanging summary care records and enabling computerized physician order entry (CPOE).

Cybercrime is an especially urgent issue. A surge in prescription drug fraud has brought steadily increasing attacks against hospitals by hackers and organized crime to gain access to prescription systems. Non-malicious security threats such as bugs and system vulnerabilities can be just as menacing, as evidenced by the notorious Heartbleed bug, which rendered hundreds of thousands of certified-secure web servers vulnerable to breach and theft. Another threat on the rise in healthcare is a type of malware known as ransomware. Ransomware, such as Locky, KeRanger, Cryptolocker, CryptoWall and TeslaCrypt, search local and network drives and encrypt critical files. The attackers, in turn, demand payment for the private key required to decrypt and regain access. Ransomware has been a plague on consumers for years, but in the last year, criminal organizations have been heavily targeting the healthcare industry.

To harness the full potential of mobility to transform the delivery of care, healthcare organizations need a holistic strategy that both enables full clinician mobility and addresses the full range of security, privacy and compliance challenges they face.

How Citrix IT solutions for healthcare promote regulatory compliance and secure clinical mobility

Citrix solutions for healthcare IT transform the clinician and patient experience, cut IT costs and accelerate organizational change while supporting security, privacy and compliance for ePHI and other sensitive data. Comprehensive, integrated technologies for mobility, virtualization, EFSS, and networking power a secure digital workspace. This portable, always-on working environment enables instant access anywhere, on any device, to complete IT resources, including not only Windows apps, but also mobile apps, EMRs and other data, with seamless roaming across devices, networks and clouds. The solution includes:

- Desktop and application virtualization powered by XenDesktop and XenApp
- Enterprise mobility management with XenMobile
- Secure file sharing with ShareFile
- Application networking with NetScaler

Citrix solutions help healthcare organizations address urgent requirements for security, privacy and compliance through a secure architecture that dramatically simplifies fundamental security functions such as data protection, access control, provisioning and secure remote access. This approach can dramatically reduce or even eliminate entirely many vexing security and compliance challenges.

Data protection

With a Citrix solution, sensitive data can be centralized in the data center and protected by a complete set of network and host security products such as next-generation firewalls (NGFWs), intrusion protection systems (IPSs), and host-based anti-malware and anti-spyware tools. These defenses are generally much more powerful and effective than the local firewall and antivirus products deployed on endpoints, and are far easier to update. Application and desktop virtualization mean that data need not be transferred from distributed workstations over the

network to the datacenter, as well as simplifying the operational aspects of data protection. In a central location it is far easier to monitor and back up apps and associated data than those residing on distributed devices. Employees are easily protected from data loss due to hardware and software failures, accidents and human errors. Data can be recovered faster in the event of a major outage or disaster. The cumulative effect is a significantly reduced attack surface resulting in reduced overall risk of data loss or data compromise.

Access control

Controlling access to applications and data residing on endpoints is extremely challenging, especially since the tools available to manage local controls vary widely across different types of laptops, tablets and smartphones. Most organizations also have multiple access points and authentication procedures to support different use scenarios based on location, device type and network. With the Citrix solution, administrators can use one set of tools to create and enforce a single set of access control policies for all users, regardless of their locations and the devices they are using.

Provisioning and de-provisioning

IT administrators need to be able to provide access to applications and data quickly as new employees and contractors come onboard, and cut off access just as quickly when they depart. Citrix technology makes it possible to provide or revoke access to applications and data on all devices a user may have used with just a few clicks, and prevent data from ever residing on user-owned devices. A self-service enterprise app store helps IT manage access while giving users fast, on-demand access to Windows applications and application updates. With convenient access to corporate-approved and tested applications, users are less likely to download potentially compromised apps from dubious app stores and compromised sites on the web.

Incident response and disaster recovery

Centralized data is easier to monitor and secure than data spread around distributed workstations. Vulnerabilities can be patched or remediated in a central location, instead of across hundreds of remote PCs and devices. In the event of an incident, such as a ransomware attack, the centralized approach enabled by Citrix solutions allows for quick containment. For disaster recovery, administrators can leverage cloud infrastructure or set up a multi-datacenter configuration where applications and data are mirrored between two sites. If one site goes down, users can quickly be switched to the other with minimal loss of data or productivity. If laptops and other devices are destroyed or unreachable in a disaster, employees can access their applications and data from other devices in safe locations.

Compliance

Auditing is a key component of compliance as well and ensuring data and systems are secure with regular reviews of access and activity. Citrix solutions provide a centralized audit trail that simplifies audits and regulatory compliance by making it simple for investigators to determine who accessed what applications and data. Not only are the systems used to access the clinical applications centralized in the datacenter, Citrix provides granular auditing for each application or desktop accessed, meaning there is no need to collect extensive logs from remote devices and provides audit data above and beyond traditional distributed infrastructure.

Empowering people throughout the healthcare delivery chain

For clinicians, a fully secure digital experience

With Citrix solutions for healthcare, IT can provide clinicians and staff with real-time access to their desktops, EMRs and key communication tools across facilities and devices without risk to patient data or professional reputation.

- Practitioners can use and roam their complete experience from any device, over any network, to email or text other members of a care team, view patient data, share documents or submit prescriptions—all without exposing sensitive data to loss or theft.
- Caregivers can access, sync and securely share files within the hospital, across the health system and to ancillary providers. Integration into Microsoft Outlook and the user's desktop allows secure file mobility without significant changes to workflow. Additionally, ShareFile's Data Loss Prevention (DLP) integration gives organizations the ability to control file sharing based on the content inside the files. With this new capability, ShareFile works with your existing DLP infrastructure to detect when sensitive content is added and lets administrators restrict access and sharing based on the results of the DLP scan.

For patients, higher-quality interactions with care providers

Patients gain a more effective care experience as clinicians are empowered to access and share information more quickly, in more places, without risk that their personal information will be compromised. Additionally clinicians are able to concentrate on the clinical experience rather than waiting on systems and applications to load, reducing IT distraction and improving quality of care.

- Patients can participate in online meetings and consultations with remote specialists through a secure online meeting solution with end-to-end encryption and meeting access control
- With instant access to the latest patient information on any device, such as a tablet they carry as they make their rounds, caregivers are able to show the latest information to their patient or the patient's family

For business leaders, better operational performance

Healthcare businesses can embrace the same approach to secure mobility trusted by more than 99 percent of the Fortune 500 to protect data while increasing productivity and agility.

- Citrix enables professionals to securely access their apps and data, share information and collaborate anywhere, on any device, rather than being constrained to fixed locations and endpoints
- To participate in health information exchanges more easily, organizations can use a network gateway to secure the information coming from the exchange without the need for site-to-site VPN or other expensive network infrastructure

For IT leaders, a more versatile, manageable and effective environment

A secure architecture makes it possible for IT to maintain a more secure and protected infrastructure even as its environment becomes more mobile by keeping data centralized in the datacenter.

- Centralized management and delivery of healthcare apps, virtual desktops and mobile services helps IT enforce comprehensive and consistent access control policies across every use scenario, including distributed outpatient and inpatient facilities.
- Desktop images and apps can be managed, patched and updated centrally, helping IT ensure that the latest security and application patches are applied quickly throughout the organization.
- IT can enable mobility while maintaining the control needed to track devices, secure access to sensitive data, and ensure compliance with HIPAA, PCI DSS and corporate policies. EMM (including MDM and MAM) provide a simple, secure mechanism to allow BYOD and BYO apps for clinicians and consultants.

- An enterprise-grade, secure file sharing solution lets healthcare providers choose where data is stored—on premise, in a dedicated healthcare cloud or in a combination of both to meet specific needs for data sovereignty, compliance, performance and cost. IT can also provide instant mobile access to data on existing network file drives and Microsoft SharePoint sites, which can't ordinarily be accessed outside the corporate network or on mobile devices. Mobile data can be managed in a secure container that can be remotely wiped by IT if needed.
- An advanced service delivery solution optimizes, secures and controls the delivery of any healthcare application, virtual desktop or mobile service. Applications and desktops run up to five times faster, ensuring that mobile clinicians can quickly access the information needed to make critical patient decisions at the point of care.

For security leaders, strict data protection and support for compliance

Citrix helps healthcare organizations protect ePHI and other sensitive data even as the IT environment becomes more diverse and mobile. Security leaders can allow mobility while maintaining the control needed to track devices, secure access to sensitive data and ensure compliance with HIPAA, PCI DSS and corporate policies.

- Virtualized desktops, applications and associated data are secure within the datacenter, protected through standards-based encryption, secure remote access, event logging and multi-factor authentication. Audit capabilities provide additional detail into usage of EMRs and other clinical applications, who sent files, when, and who received the file.
- Instead of sharing information via email and portable storage devices—a common cause of data leakage, compliance issues and a potential vector for attack—organizations can empower users with a secure enterprise file sync and share service that ensures full security and auditability without changing workflows.
- Integrated app container technology for mobile devices enables data encryption, password authentication, secure lock and wipe, inter-app policies and micro VPNs to mobile apps. IT can determine the applications their controlled apps can interact with, and can remote-wipe corporate data only, leaving the user's personal data untouched.
- A secure front end for web properties with the fastest web app firewall available protects web servers from malicious traffic and data breaches, and protects the back end system from compromise.

How leading healthcare organizations are using Citrix Healthcare IT solutions today

Southcoast Health System

Southcoast Health System is a not-for-profit healthcare provider headquartered in New Bedford, Massachusetts, with three hospitals, 27 physician offices, a cancer center, urgent care facilities, labs and radiology centers, and a visiting nurse service. As its organization grew rapidly, Southcoast needed to ensure the security of PHI while delivering seamless access to patient records across facilities and devices.

Citrix Healthcare IT solutions enabled Southcoast to provide secure, uniform access to health records by physicians and nurses—whether they use PCs or laptops, at their practice or in the hospital. Southcoast chose Citrix XenDesktop and XenApp virtualization software as the foundation to deliver its integrated EMR system as well as 50 other clinical and nonclinical applications. Citrix NetScaler serves as the front end for the environment, providing granular secure access control while maintaining reliable high performance for web-based applications. Citrix XenMobile provides complete enterprise mobility management (EMM) functionality, helping the organization manage and secure apps and data on users' mobile devices. The new infrastructure protects against data leakage and controls the influx of new mobile devices, even when clinicians bring their own devices, helping Southcoast keep patient data safe and ensuring that sensitive information remains private.

Said Mark Lacombe, Director of Information Technology at Southcoast Health System, "Citrix XenMobile handles mobile device management as part of the application, and it also has the flexibility to support our bring-your-own-device policies," he says. "We can lock devices, wipe data, upgrade and manage devices, and be proactive in case of a security incident—all while creating an intuitive experience for users."

Franciscan Missionaries

Franciscan Missionaries of Our Lady Health System (FMOLHS) is a nonprofit, mission-focused Catholic health system headquartered in Baton Rouge, Louisiana. Previously, FMOLHS had shared desktops on each hospital floor where any employee could walk up and log in. A clinician could accidentally save a file with a patient's PHI to the shared desktop, unintentionally enabling another user to access it at a later point. This posed a significant risk of a HIPAA breach. FMOLHS needed a more secure way to deliver EMRs in both inpatient and ambulatory settings to meet meaningful use and CPOE requirements, while avoiding lapses in compliance. The right solution would also enable FMOLHS to address device proliferation and rising requests for BYOD.

FMOLHS now provides employees and contractors with an end-to-end mobile workspace powered by XenDesktop virtual desktop infrastructure (VDI) and application virtualization; XenMobile, which includes secure productivity apps for mail, calendar, browser, notes and more; ShareFile for secure enterprise file sync and sharing; and NetScaler for application delivery and secure access control.

With its new digital workspace from Citrix and two-factor authentication (badge and PIN) from Citrix partner Imprivata, FMOLHS no longer has to worry about potential breaches on shared desktops. The organization now delivers seamless roaming with logins in under five seconds, allowing clinicians to simplify workflows, improve satisfaction and meet CPOE requirements. The solution also enabled IT to address a technology executive's request for BYOD support in less than two weeks.

Said Johnny Brister, manager of infrastructure and technology systems, FMOLHS, "We've used Citrix to implement security controls and prevent breaches from occurring. XenApp, XenDesktop and XenMobile have all been critical in how we deliver essential applications or services while maintaining a very high level of security."

Nicklaus Children's Hospital

Founded in 1950, Nicklaus Children's Hospital (NCH) is renowned for excellence in all aspects of pediatric medicine with several specialty programs ranked among the best in the nation by U.S. News & World Report. As a world-class pediatric hospital with a goal to be able to provide care to any child, at any time, anywhere, NCH needed a way to make content, from patient data and lab reports to surgical best practices, available when and where it's needed while maintaining security and compliance.

NCH has used Citrix Healthcare IT solutions to build a secure telehealth infrastructure that protects patient information wherever its doctors deliver care. XenDesktop and XenApp make virtual desktops and applications available securely on any device, including EMRs powered by Cerner. XenMobile ensures the security of corporate email and patient consent forms on mobile devices.

Clinicians can now log into desktops and apps quickly and securely on any device to access the information they need to guide the care they provide. Wherever and however this content is accessed, it remains secure and protected within the datacenter. Said Ed Martinez, senior vice president and CIO, NCH, "Our Citrix-powered secure telehealth platform has seamlessly

integrated and operationalized capabilities to enable doctors to consult with, diagnose and prescribe treatment for remote patients as if they were in the same room, while protecting their PHI wherever it is accessed."

Conclusion

A digital workspace can have a transformative impact on the ability of a healthcare organization to deliver care—but it must be implemented with the security and control needed to protect ePHI and maintain compliance. Citrix solutions for Healthcare IT make the full benefits of digital transformation available to every member of the healthcare ecosystem, including clinicians, patients, business leaders, IT leaders and security leaders. Citrix solutions provide anywhere, any-device access to complete clinical apps, data and patient information, powered by comprehensive technologies for desktop and app virtualization, enterprise mobility management, secure file sync and sharing, and application networking. As a result, healthcare organizations can optimize their delivery of care, improve satisfaction and work-life balance for practitioners, increase operational efficiency and empower collaborative, seamless, patient-centered care across entities and locations. As the experiences of South Coast Health System, Franciscan Missionaries of Our Lady Health System and Nicklaus Children's Hospital demonstrate, secure mobility in healthcare is both entirely possible—and increasingly essential for meeting the requirements of today's healthcare environment.

Additional resources

For more information, please look at these additional resources:

Web

Citrix Solutions for Healthcare
Citrix Solutions for Security and Compliance

Solution brief

Citrix Solutions for Healthcare and HIPAA Compliance

CITRIX®

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309 United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054 United States