Manage endpoints to improve healthcare service delivery

As data and mobility grow, it is more important than ever for healthcare organizations to actively manage their full range of endpoints

IBM

Contents

Introduction

There is no question where healthcare information, applications, collaboration and insight are going. They are going straight to the bedside, the examining room, the patient's home—and wherever else they are needed.

Already, 83 percent of healthcare organizations support the use of tablets on their networks—and 60 percent support electronic medical record applications on mobile devices.[1] Among physicians, the use of tablets has jumped dramatically, reaching 62 percent in 2012, double the rate of only a year earlier.[2]

At the root of this growth is the ability to improve patient care with the fast and simple information access, communications and record keeping of these touchscreen devices. There is also the convenience. Unlike a laptop, a number of tablets fit perfectly into the pocket of a lab coat.[3]

But adopting mobile technology is not as simple as putting a device in a pocket. Information access involves endpoints of all kinds, from mobile devices to desktops to servers. And like the complex human organisms the healthcare industry serves, there is a lot going on "under the skin" in healthcare IT to bring information access to life.

Healthcare organizations must provide connectivity in environments filled with conflicting electronic signals, control role-based application access, ensure security of patient data, comply with strict government regulations—and much more. These organizations, as a result, are increasingly turning to comprehensive endpoint management solutions that can address their complex, device-related challenges.

This white paper will discuss the growing need for unified, cross-organizational endpoint management, issues such as security and regulatory compliance surrounding these management capabilities—including those created by the increasing use of mobile computing—and solutions for providing secure, scalable, streamlined IT capabilities to control all endpoints in healthcare environments.

Properly managed endpoints provide clinical, business and IT advantages

Driven by the severity and high costs of chronic diseases such as diabetes and obesity; the changing demographics of an aging population; and patient expectations for improved communication with providers, better access to medical information, and an increased role in their own care, today's healthcare organizations face pressing needs for change. Many are responding with innovative programs for mobile as well as fixed information access.

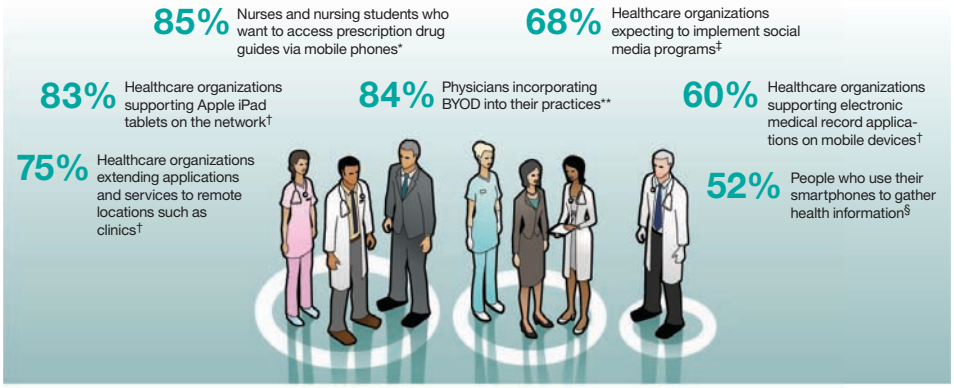
One provider is piloting an initiative to improve patient outcomes with remote healthcare support. Its home care program provides diabetes patients with Apple iPad tablets they can use to reduce onsite visits by inputting their own diagnostic data and conducting video consultations with doctors and nurses. Another program provides the parents of babies in the neonatal intensive care unit with iPod Touch devices pre-loaded with educational applications to assist with care.

But how do you arrive at such advanced mobility? How does a healthcare organization move from recognizing a need to actually implementing solutions that improve patient care and streamline hospital functions?

The challenges presented by heterogeneous and widely distributed infrastructures, stringent regulations requiring data security and confidentiality, a proliferation of mobile endpoints—including endpoints owned by employees—and the need for intelligent and scalable device management can be daunting.

Properly managed mobile and fixed endpoints, however, can help healthcare organizations gain the clinical, business and IT agility they need to meet evolving patient needs and market demands. Effective management can help ensure the security necessary for cross-departmental collaboration. It can provide unified control of all technology endpoints, from smartphones, tablets and laptops to desktops and servers. And it can provide multi-sourced information to support analytics and insight that the organization can use to improve the delivery of healthcare services.

Information access trends in healthcare



* Sara Jackson, "BYOD continues to challenge hospitals' security boundaries," *FierceMobile Healthcare*, May 14, 2012.
** Michelle McNickle, "BYOD Security Tops Doctors' Mobile Device Worries," *InformationWeek*, October 31, 2012.
† "2012 Healthcare Mobility Trends Survey Results," *Aruba Networks, Inc.,* Sunnyvale, CA, 2011.
‡ Penny Schlyer, IBM Software Group, "Healthcare leveraging big data for social business," *IBM Social Business Insights Blog,* September 26, 2012.
§ "Mobile Health 2012," *Pew Research Center Internet & American Life Project*, Washington, D.C., November 8, 2012.

Soaring growth in data brings rapid change in endpoint use

According to a recent IBM study, nearly half of chief information officers (CIOs) in healthcare agencies have been given the mandate to help re-engineer their organizations to make them faster, more flexible and more able to turn data into insights.

And nearly a third have been charged with transforming their organizations to make stronger connections with patients and other key stakeholders.[4] Another IBM study found that top healthcare leadership strongly supports increased collaboration and partnerships to enhance institutional innovation.[5]

These trends and initiatives can have a significant influence on an organization's choice of endpoint technologies—and on the clinical, business and IT use and support of those technologies. But healthcare leadership is not alone. That is because when it comes to deploying and supporting endpoints in healthcare, myriad trends, preferences, challenges and strategies from industry, government, the public and the care providers themselves also come into play.

In the communications industry, for example, some 78 percent of executives see healthcare as the top growth opportunity for their mobile 4G services.[6] In government, a recent proposal would create new initiatives to advance innovation in mobile and other healthcare technologies.[7] And among the public, 52 percent of smartphone owners gather health information on their phones—while 19 percent have at least one health-related application installed on their phones.[8]

This soaring growth in digital information—the amount of data managed by healthcare providers in North America alone is expected to more than quadruple its 2010 levels by 2015[9]—and the corresponding need for information access has brought dramatic change in both the clinical and business use of healthcare resources. It also has brought change in the adoption of endpoint devices for accessing those resources. Today, 75 percent of healthcare organizations extend access to their applications and services to remote locations such as clinics or affiliated physicians' offices.[1] Some 68 percent of healthcare chief executive officers (CEOs) are planning to use social media to engage patients and other stakeholders—and a similar number plan dramatic improvements in both internal and external collaboration.[10]

In healthcare, endpoint management must create a careful balance

Managing endpoints to meet the challenges of increased mobility, connectivity and access requires a carefully balanced approach. In delivering high-quality service, for example, physicians, nurses and the clinical staff require high system availability and rapid data access—but government regulations and sensitivity to patient privacy require high levels of security and confidentiality. Meanwhile, the organization's business departments need secure and reliable access to support both internally facing administrative processes and externally facing patient interaction. And IT needs infrastructure-wide visibility and automation to support diverse endpoints—whether mobile smartphones and tablets or conventional laptops, desktops and servers—and the heterogeneous environments in which they operate.

Endpoint management, as a result, is of utmost importance to all operational functions of healthcare organizations. On today's smarter planet, the increased instrumentation, higher use of digital technology and rapid proliferation of mobile devices in clinical scenarios are making possible the smart use of healthcare information and the game-changing innovations that support better care. Challenges such as the pervasive need for security, the growing cost of processes and systems, and the increasing complexity of IT, however, also demand a smarter approach to managing endpoint devices in both clinical and business environments.

Leadership initiatives in evolving healthcare

60% Healthcare CEOs actively working to improve internal collaboration*

53% CEOs forming external partnerships to improve innovation*

45% CIOs tasked with helping to re-engineer healthcare organizations†

29% CIOs charged with improving connections with patients and stakeholders†

* IBM Institute for Business Value, "Leading Through Connections," *IBM Global CEO Study 2012,* May 2012.

† IBM Institute for Business Value, "The Essential CIO," *IBM Global Chief Information Officer Study*, May 2011.

Effective endpoint management spans the entire healthcare organization

Early adopters of electronic medical records and other methods of digitally recording, storing and accessing information relied on laptop and desktop systems—with some desktops even installed on carts that could roll to labs or patient rooms to support care where it was needed. To ensure security as they transmitted patient records across the network, these systems utilized encryption. With true mobility provided by a more heterogeneous set of endpoints and applications, however, using endpoints in patient care is touched by a wider range of applications, information sources—and challenges.

The issues that IT must address in enabling endpoints go beyond basic encryption to ensuring compliance with security, regulatory and operational policies. They reach beyond the patient records on the network to Internet-based sources of information created and provided specifically for clinicians. And they extend beyond the institution's own walls to connect with remote offices, environments with varying degrees of bandwidth and remote users who work both on and off the network.

The resulting need for effective endpoint management requires scalability and flexibility as the numbers and types of users and endpoints increase. And it requires automation, as infrastructure complexity and the IT workload grows. It must reliably support high availability in critical healthcare scenarios. And it must ensure data security, information confidentiality and compliance with regulations such as those established by the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH) or the European Medicines Agency (EMA).

These requirements are made still more challenging by the complex heterogeneous and legacy environments in which endpoints operate. Healthcare endpoints often include a wide variety of legacy servers and desktops, as well as laptops, tablets, kiosks and wireless/mobile diagnostic equipment. They typically run a variety of operating systems, including Microsoft Windows, Linux, UNIX and Mac OS. A healthcare organization with a limited IT staff and budget can feel overwhelmed by responsibilities that have grown so large and complex.

Clinical requirement: Security and compliance

In Washington D.C., a laptop containing nearly 35,000 patient records was stolen from a hospital contractor's vehicle. In California, nearly 32,000 patient records in a regional health system were exposed to a possible security breach by errors in system security settings. In Utah, health information on some 780,000 Medicaid patients and recipients was stolen from a state government agency by a computer hacker taking advantage of a weak password.[11]

In healthcare, avoiding data breaches such as these is not only good business practice, it is the law. Failure to demonstrate compliance can not only impact functional operations, it can result in fines and penalties. The odds of data being stolen or compromised increase when data resides on a mobile device that may leave the premises—but breaches such as hacking can occur anywhere. The challenge, then, becomes securing and managing the institution's wide range of endpoints, including those that are owned by employees and used at work under "bring-your-own-device" (BYOD) initiatives. An effective solution will ensure security configurations and other protective measures, streamline and simplify patching of application vulnerabilities, support compliance reporting, and assist with remediation in case of an attack.

Clinical requirement: Information access

Doctors, nurses and other clinical professionals need fast, simplified information access, whether it is to network-based patient records or Internet-based prescription drug and other diagnostic information. Insights delivered via smartphone or tablet directly to the bedside, rather than later to an office-bound PC, can be invaluable in ensuring high-quality patient care—but time is often short and access must be uninterrupted, even in low-bandwidth, high-latency environments. An endpoint management solution must be able to enforce security measures without reducing or slowing access. To ensure availability, the healthcare organization must not take up excessive bandwidth with system management tasks such as software distribution or endpoint discovery. And Wi-Fi networks must be up and running at full strength 24x7.

Clinical requirement: Device sharing

In a clinical setting, it is not unusual for staff to share devices. In a hospital's around-the-clock shifts, for example, a tablet computer can pass through multiple hands in the course of a day. As a result, users must not only be assured of security and high availability, they must also be provided with individual logins, applications and access to patient records in order to meet specialized aspects of their jobs. Similarly, an institution may provide devices to doctors or nurses who carry them to branch clinics. Or affiliated clinicians may use their own devices on the institution's Wi-Fi network. Each of these scenarios requires a management system that is robust enough to handle the complexity of multiple shared and roaming devices—and one that provides IT with ease-of-use features that help reduce the management workload.

Business requirement: Secure BYOD

In healthcare organizations, BYOD scenarios are more likely to occur in the business and administrative divisions than in the clinical ones. This is because business and administrative employees typically are not accessing sensitive information regarding patient health, which must be carefully protected. They do, however, often handle other patient information, such as social security numbers, so security measures such as proper device configuration still must be followed to guard against data theft—and capabilities such as remote wipe should be provided in case a device containing data is lost.

Business requirement: Controlled costs

With the cost of healthcare continuing to rise, any measures an organization can take to control expenses without reducing quality of care can benefit both the business and its stakeholders, including patients. An endpoint management solution that automates IT processes can save costs by reducing the IT workload and decreasing the need for new equipment. A unified device management and security solution can help ensure productivity of staff throughout the organization with the security, availability, flexibility and access that modern healthcare delivery demands.

IT requirement: Streamlined management

A healthcare organization's endpoint management needs are as wide-ranging as the devices used by clinical and business staff and as mission-critical as the patient care the organization delivers. Endpoint management can ensure connectivity is available

across the facility—mobile devices can, in fact, be used to monitor network quality of service and to help resolve weaknesses that limit data access. And it can speed software distribution—a streamlined management solution can roll out electronic health record systems or complex applications in weeks rather than months or even years.

A complete endpoint management solution can also enable healthcare providers to gather a full inventory of all connected devices and all authorized and unauthorized software in the network—and then quickly and seamlessly remove any unauthorized software it finds. It can secure configurations on iOS, Google Android and Windows operating systems—and ensure that all operating systems meet standards. It can create custom policies to remediate and help prevent future system vulnerabilities. With an endpoint management solution, a healthcare organization can change passwords, change user groups and delete unauthorized users. It can monitor sensitive information and discover any unauthorized attempts to remove sensitive data.

IBM Endpoint Manager in healthcare environments

- **Concord Hospital in New Hampshire used IBM® Endpoint Manager to simplify IT operations and provide visibility into its IT environment—eliminating malware infections, increasing patch compliance from 60 to 93 percent and accelerating system maintenance.**
- **Christian Hospital Centre in Belgium used Endpoint Manager not only to halt attempted intrusions before they penetrated the infrastructure, but also to anticipate future threats. The solution enables near real-time remediation for any endpoint issues that do occur.**
- **St Vincents and Mater Health Sydney in Australia used the patch management, configuration compliance, power management and asset discovery capabilities of Endpoint Manager to achieve visibility and control over 100 percent of its endpoints, mitigating risk and reducing costs.**

Conclusion

IBM Endpoint Manager, built on IBM BigFix® technology, can help healthcare organizations effectively and efficiently manage both fixed and mobile endpoints as it helps meet stringent healthcare industry regulations. Designed to keep endpoints secure, compliant and running at peak performance, Endpoint Manager can unify the management of up to 250,000 PCs, Macs, servers, kiosks, smartphones, tablets and more from a single console and server.

Providing enterprise-wide, real-time visibility over all endpoints—regardless of their location, bandwidth or network connectivity—Endpoint Manager enhances day-to-day operational productivity as it supports compliance with regulatory requirements such as HIPAA and HITECH.

Quickly addressing the unexpected—such as "zero-day" attacks—Endpoint Manager enables rapid and simplified responses to threats, remediating, protecting and reporting on endpoints in real time.

Collapsing management actions from months or weeks to days or hours—patch and inventory cycles, for example, can be completed in only hours with 98 to 99 percent first-pass success—Endpoint Manager delivers significant capabilities to reduce management complexity and cost, increase accuracy and reduce the IT workload in busy healthcare environments.

Additionally, environments utilizing IBM Netcool®/OMNIbus can better handle the additional management load from mobile devices—without upgrading the network—when they deploy Endpoint Manager for wireless visibility and control.

For more information

To learn more about IBM Endpoint Manager, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/tivoli/endpoint

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

[1] "2012 Healthcare Mobility Trends Survey Results," *Aruba Networks, Inc.*, Sunnyvale, CA, 2011.

[2] "New Study Reveals Physicians' Device and Digital Media Adoption Rapidly Evolving," *Manhattan Research*, New York, May 10, 2012. http://manhattanresearch.com/News-and-Events/Press-Releases/physician-digital-media-adoption

[3] Lucas Mearian, "Doctors prescribe iPad Mini: a perfect lab coat fit," *Computerworld*, November 9, 2012. http://www.computerworld.com/s/article/9233431/Doctors_prescribe_iPad_Mini_a_perfect_lab_coat_fit

[4] IBM Institute for Business Value, "The Essential CIO," *IBM Global Chief Information Officer Study*, IBM Corp., May 2011.

[5] IBM Institute for Business Value, "Leading Through Connections," *IBM Global CEO Study 2012*, IBM Corp., May 2012.

[6] "Mobile industry views health care as growth opportunity," *iHealthBeat*, March 22, 2012. http://www.ihealthbeat.org/articles/2012/3/22/mobile-industry-views-health-care-as-growth-opportunity.aspx

[7] "Bill aims to advance innovation in mobile health technology," *iHealthBeat*, December 5, 2012. http://www.ihealthbeat.org/articles/2012/12/5/bill-aims-to-advance-innovation-in-mobile-health-technology.aspx

[8] "Mobile Health 2012," *Pew Research Center Internet & American Life Project*, Washington, D.C., November 8, 2012. http://pewinternet.org/~/media//Files/Reports/2012/PIP_MobileHealth2012_FINAL.pdf

[9] John McKnight and Brian Banineau, "North American Health Care Provider Information Market Size and Forecast," *Enterprise Strategy Group*, Milford, MA, January, 2011.

[10] Penny Schlyer, IBM Software Group, "Healthcare leveraging big data for social business," *IBM Social Business Insights Blog*, September 26, 2012. https://www-304.ibm.com/connections/blogs/socialbusiness/entry/healthcare_leveraging_big_data_for_social_business10?lang=en_us

[11] Michelle McNickle, "Top 10 data security breaches in 2012," *Healthcare Finance News*, June 12, 2012. http://www.healthcarefinancenews.com/news/top-10-data-security-breaches-2012

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2013

TIW14152-USEN-00