SOTI

ENTERPRISE MOBILITY MANAGEMENT

Healthcare's Painful Choice: Convenience vs. Compliance

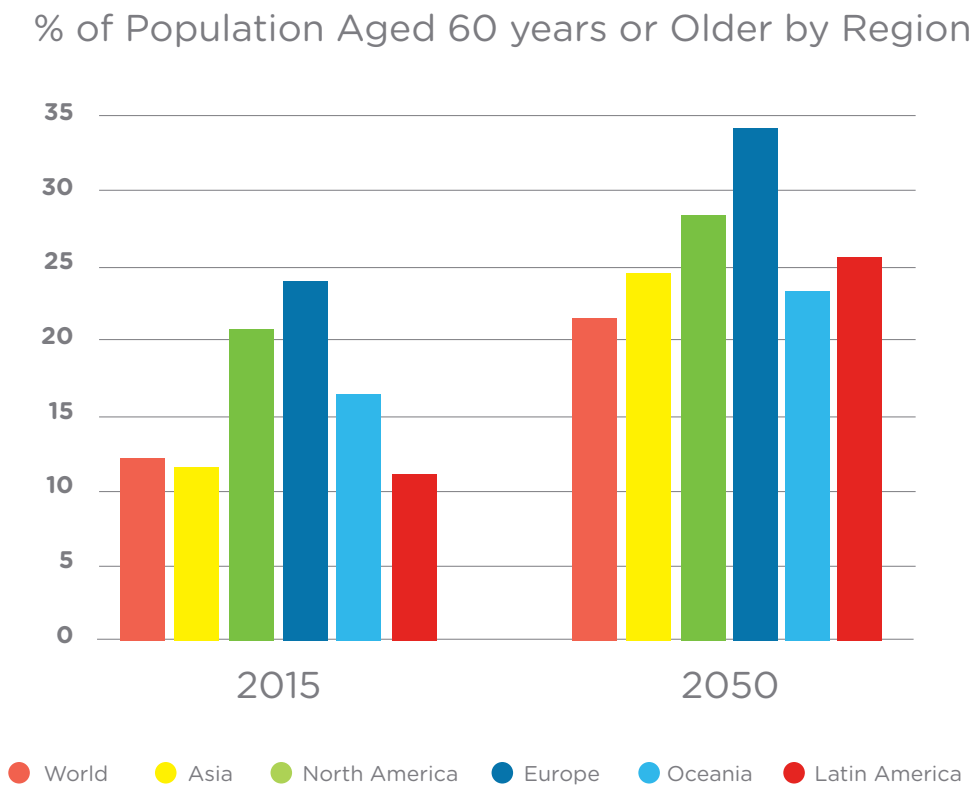
Around the world, people are living longer – often with chronic disease. This is increasing the demand on healthcare systems at the same time that many are experiencing shortages of qualified personnel. In response, hospitals are aggressively deploying mobile devices and applications to increase the efficiency and effectiveness of their workers, and deliver high-quality patient care. However, unsecured mobile technology is risky. Healthcare organizations are being forced to choose between the convenience of mobile technology and the legal requirement for compliance and patient data privacy.

contents

The global population is getting older

Declining fertility and increasing longevity are rapidly aging the world's population. The UN* predicts that the number of people aged 60 and over will grow from 900 million in 2015 to nearly 2.1 billion by 2050. Furthermore, the share of the **oldest** population, 80 years and over, will more than double by 2050.

The growing number of older (and oldest) people will require an increase in the prevention, treatment and ongoing management of many health issues associated with old age. At the same time, environmental conditions and lifestyle choices are contributing to an upswing in chronic and non-communicable diseases. This means that many healthcare systems that are already at capacity will be overwhelmed by an increase in the geriatric population and their growing need for health care.



*UN World Population Ageing 2015

SOTI

Fewer healthcare practitioners are available

Just as the demand for healthcare is ramping up, many countries and their healthcare systems are experiencing a shortage in physicians, nurses and allied health professionals. The World Health Organization (WHO) forecasts a global deficit of almost 13 million trained health professionals by 2035*. Developing countries are even more at risk — few are able to meet the basic WHO threshold of 22.8 health professionals (physicians, nurses and midwives) per 10,000 population and for many countries this ratio is on the decline.

- By 2025, the U.S will have a physician shortage ranging between 61,700 and 94,700.**
- In 2016, the National Health Service (NHS) in the U.K., estimated there were 23,443 nursing vacancies and 6,207 doctor vacancies in England, Wales and Northern Ireland.
- India has over 400 medical schools, but still has a shortfall of over 750,000 doctors.

*World Health Organization, 2013- A Universal Truth – No Health without a Workforce
** American Association of Medical Colleges (AAMC)

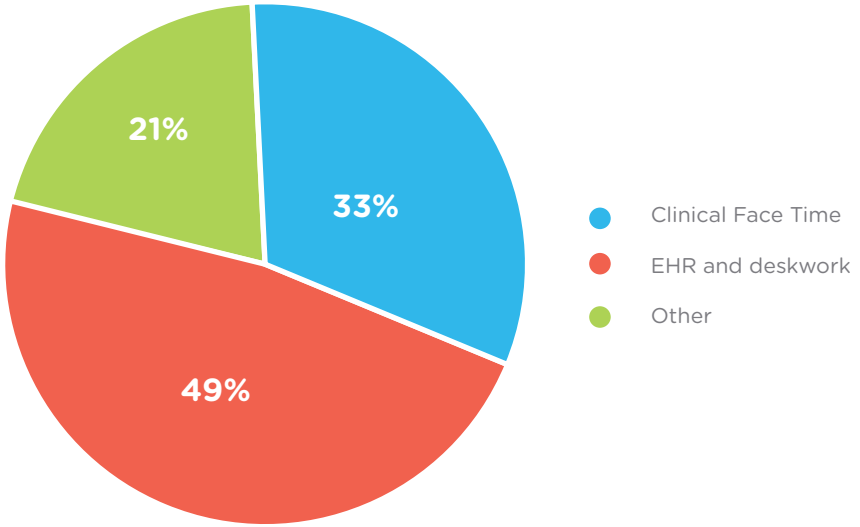
SOTI

Too much time spent on administrative work

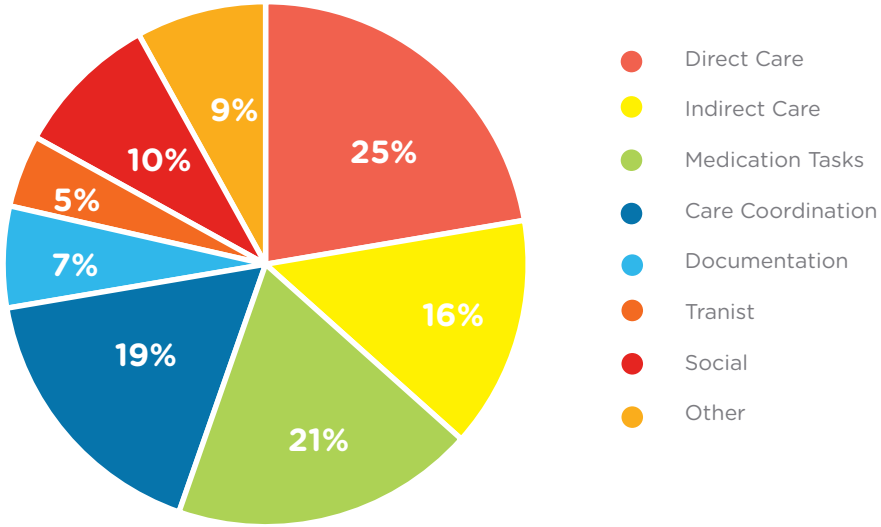
Hospitals are deploying Healthcare Information Systems (HIS) to improve clinical workflows and reduce potentially lethal medical errors. Even so, physicians and nurses are spending more and more of their day dealing with administrative duties and non-clinical activities. A recent, multi-specialty time and motion study* found that physicians spend almost 50% of their time doing deskwork and updating the Electronic Health Record (EHR), while only 33% of their time was spent clinically with patients. The results for nurses were similar** – they only spend 37% of their time interacting with patients, and much more time accessing the HIS to update medical records, manage medication, and communicate with other medical personnel.

There is considerable evidence that medical practitioner job satisfaction, and patient outcome, is correlated with the amount of time healthcare workers are able to spend with patients. Too much admin work can result in burnout and compassion fatigue, which in turn leads to disengagement and decreased patient satisfaction.

Physician Time Distribution



Nurse Time Distribution



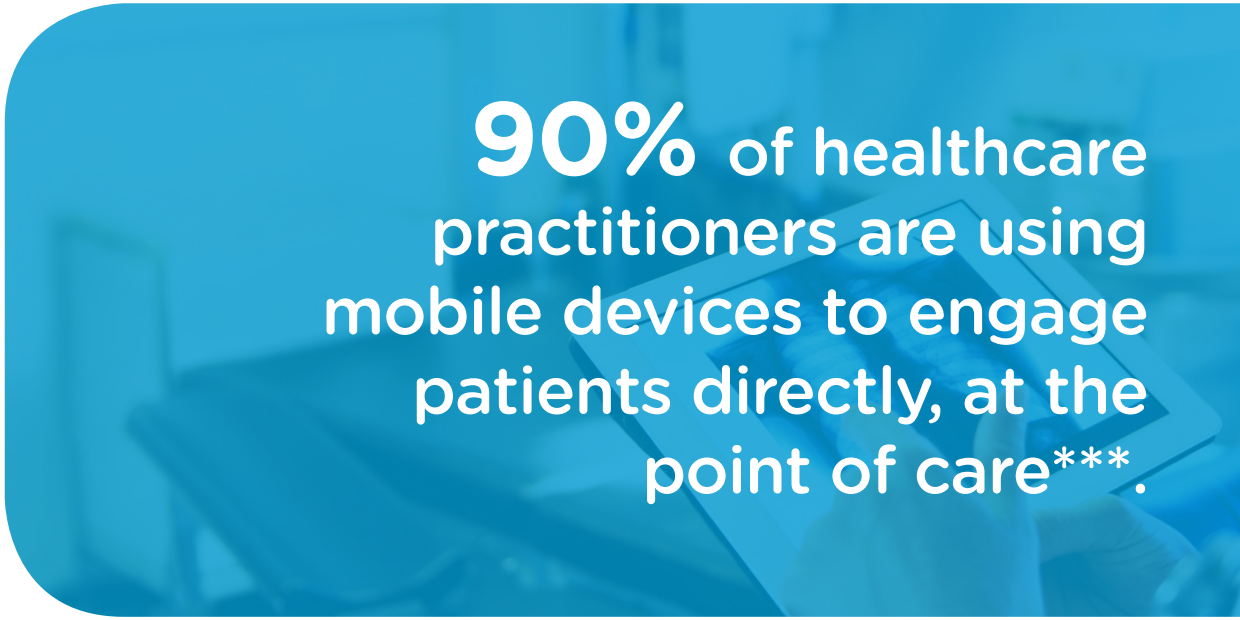
*Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in four Specialties - Annals of Internal Medicine, September 2016
**How much time do nurses have for patients? A longitudinal study quantifying hospital nurses' patterns of task time distribution and interactions with health professionals - BMC Health Services Research, November 2011

SOTI

Healthcare organizations are embracing mobile technology

Healthcare organizations are turning to mobility solutions to increase worker productivity. A recent report* predicts that the global healthcare solution market will grow from approximately $20 billion in 2015 to almost $150 billion by 2023. A significant part of this growth is the mobile devices segment.

Even more importantly, healthcare organizations are starting to take a more rational approach to enterprise mobility. A recent survey** found that 63% of healthcare organizations have a documented mobility strategy, while an additional 12% are in the process of creating one. This is a significant improvement from just a few years previously when only 34% of healthcare organizations had a documented mobility strategy in place. The devices that these organizations are supporting within their mobility strategy include smartphones, pagers, WiFi phones, tablet computers, voice badges, and wearables.



*Transparency Market Research - Sept 2016 - Healthcare Mobility Solutions (Payers, Providers, and Patients (Individuals)) Market - Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2015 – 2023
**SPOK's Fifth Annual Mobility Strategies in Healthcare Survey
***2015 HIMSS Mobile Technology Survey

SOTI

How are healthcare workers using mobile technology?

A 2014 report from Epocrates*, finds that 100% of clinicians (physicians, nurse practitioners, and physician assistants) used a personal computer, 80% used a smartphone, and 45% used a tablet computer in a professional capacity.

Healthcare workers are using mobile devices for:

- Communication & collaboration — Voice, video conferencing, text, and e-mail
- Accessing Healthcare Information Systems — Electronic health / medical records (EHR & EMR), Picture archiving and communication systems (PACS), Computerized physician order entry (CPOE), and Laboratory information systems (LIS)
- Informational resources — Medical research, drug information, medication side effects and drug interactions
- Clinical software applications —Remote monitoring, disease diagnosis aids, dosage calculators, order sets and clinical pathways

Portability vs. Mobility

Laptop PC's and Computers on Wheels (COWs) have been used by healthcare workers for years. They provide secure access to important HIS solutions at the patient bedside, the nurse's station and/or the doctor's office, but NOT in between. These devices are portable, not mobile.

Smartphones and tablets deliver a powerful, mobile computing experience from anywhere and anytime. This immediacy improves productivity, reduces errors and keeps workers happy and engaged.

80% of physicians use a smartphone in a professional capacity*

*Epocrates – 2014 Mobile Trends Report

SOTI

Non-clinical devices and applications streamline operations

For many CIOs, mobile devices and applications have the potential for equal or greater impact on NON-clinical workflows and hospital operations. Some of the high-impact areas include:

Self-Registration Kiosks	Tablets and touchscreen computers reduce staff workload, makes the patient registration process faster, and reduces data errors.
Logistics for Porters	Remotely allocate tasks to porters based on location, priority and current workload. This reduces delays, improves porter utilization, and provides improved visibility and reporting.
Appointment scheduling	Mobile applications make it easier for patients to schedule appointments with physicians, therapists and medical services.*
Wayfinding / Navigation	Mobile applications and kiosk technology help patients and their families navigate around the hospital and locate POIs such as ATMs, gift shops and food courts.**
Hospital Maintenance	Computerized maintenance management system (CMMS) schedule, assign, and track maintenance work orders.

*San Diego Tribune – November 9, 2016 - VA to launch online appointment scheduling

** PR Newswire – November 2016 - Overlook Medical Center Launches New App with Indoor GPS for Patients and Visitors

Patient data privacy around the world

Most developed countries have well established data privacy regulations, while others regulate data by industry or demographic. For example, the U.S.A. does not have a single overarching data privacy law, but it does have the Healthcare Insurance and Portability Accountability Act (HIPAA) for controlling personal health information data and the Children's Online Privacy Protection Act (COPPA) to protect the personal information of children under 13. Unfortunately, there are many parts of the world with only rudimentary protection of personal data.

Australia

Australia's Privacy Act, enacted in 1998, regulates the handling of personal information by government agencies and private sector organizations. In addition, the My Health Records Act (2012) and Rule (2016 amendment) regulate when and how health information can be collected, used and reported.

Canada

The Personal Information Protection and Electronics Document Act (PIPEDA) passed in 2008. It defines a set of standards that both safeguard the personal data of Canadian citizens and allow businesses reasonable access and use of the data to achieve business ends.

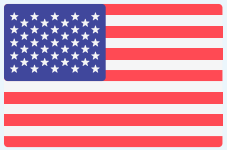
Europe

The General Data Protection Regulation (GDPR) passed in 2016 supersedes the 1998 Directive on Data Protection. The primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

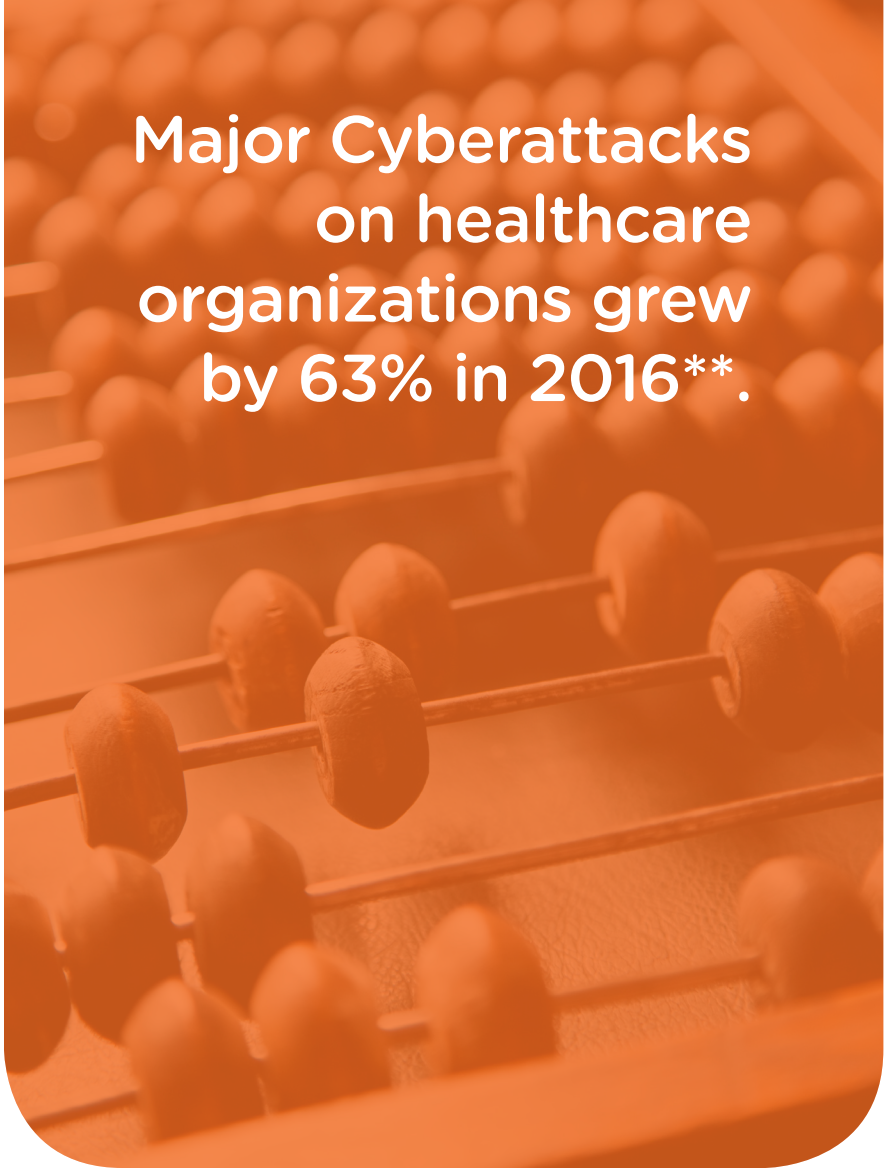
India

The Information Technology Act (2000), was amended by the Information Technology (Amendment) Act (IT Act) in 2008. The IT Act penalises "cyber contraventions" (extracting data from unauthorised computer systems or networks) and "cyber offences" (hacking with intent to cause damage and breach of confidentiality and privacy).

USA



The Health Insurance and Portability Accountability Act (HIPAA) was enacted by congress in 1996. Title II of HIPAA defines policies, procedures and guidelines for maintaining the privacy (The Privacy Rule) and security (The Security Rule) of individually identifiable health information, termed Protected Health Information (PHI).



How common are healthcare data breaches?

Healthcare has gained the reputation of being the 'leakiest' industry when it comes to data privacy. Unfortunately, this reputation is expected to get worse — the carelessness of healthcare workers is now overshadowed by cybercriminals actively targeting healthcare organizations. Every year there are more hacking and phishing attacks and unfortunately, they are increasingly subtle and effective.

- From 2015 to 2016, there was an 88% increase in the number of data breaches reported to the U.K's Information Commissioners Office (ICO)*. The healthcare industry recorded the highest number of breaches, 941.
- In 2016, there were approximately 330 significant breaches reported to the U.S. HHS**, that unlawfully disclosed personal information from over 16.5 million individuals.
- In October 2016, the Australia Red Cross was hit with a record-breaking data breach of almost 1.3 million donor records going back six years. The leaked data included a significant amount of PHI, including name, gender, address, email, DOB, and phone number.

*The Register – September 2016

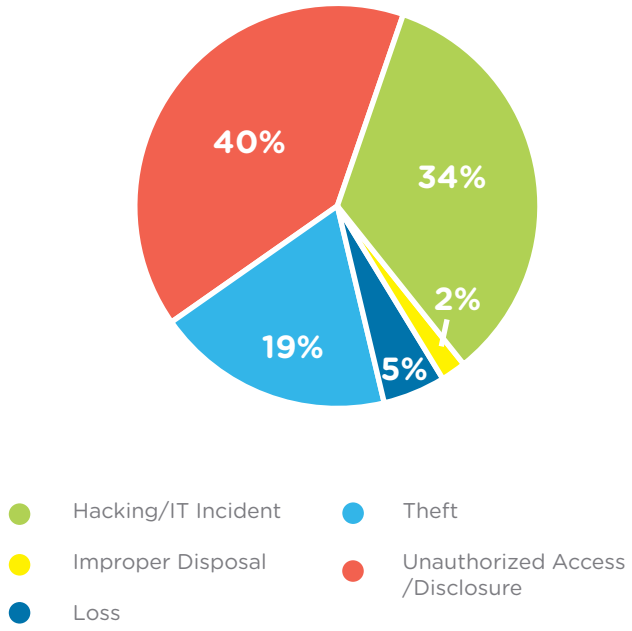
**US Department of Health and Human Services (HHS) Breach Portal

Common threats to healthcare data privacy

The actual numbers may vary from country to country, but the cause of healthcare data breaches is very consistent. A more detailed analysis of the 330 data breaches reported to the U.S in 2016 shows five major causes:

Improper Use / Disposal	Mishandling of medical records was more common when medical records were paper and could be left in a patient room or exam room, but even in the era of the Electronic Medical Records, organization need to be careful how their employees are handling patient records – how and where they are accessed, filed and archived.
Unauthorized access / disclosure	Inadvertent disclosure such as conversing about a case while standing in line at the hospital coffee shop or at a social gathering can reveal important information to bystanders. Using SMS, MMS or other messaging programs to send test results or discuss patient status may seem innocent, but it can leak PHI to someone with malicious intent.
Theft	As enterprise mobile devices have shrunk in size and grown in capabilities, they are increasingly target of theft. When you consider that as many as 14% of doctor devices are completely unsecured*, it is an easy way for criminals to access patient data, or even the hospitals secure HIS systems.
Loss	Everyone has lost their mobile device at some point or other. Whether it is only for a couple of hours or for good, those devices present a risk of data loss.
Hacking / IT Incident	Increasingly, healthcare system are being targeted by cybercriminals to either steal patient data, or lockdown the system and extract payment, commonly called Ransomware.

PHI Breaches Reported - 2016



*DarkReading, April 2016 – Doctors' MobileDevices Putting Patient at Risk

**US Department of Health and Human Services Breach Portal

SOTI

The consequences of data privacy breaches

Exposed patient data affects both the individual whose data is leaked, and the business where it leaked from. This impact is exacerbated by any delay in informing the patient, but some regions or countries that have strict data privacy legislation do not have timely reporting requirements. Identity theft is the major concern of the individual. Regaining control of their identity can be very stressful and expensive in terms of time and dollars.

For the hospital or healthcare organization, the cost and consequences of healthcare data breaches can be quite significant. In addition to lost customers, remedial action can include litigation, engaging forensic experts and performing security audits. A 2016 report* indicates that data breaches in the healthcare industry are the most expensive at approximately $355 per record globally. Based on breach size and frequency, the average total cost of a data breach increased to $4 million in 2016.

What is **Electronic Protected Health Information** (ePHI)?

- Names
- Birth dates, death dates, treatment dates, admission dates and discharge dates
- Telephone numbers and other contact information
- Addresses
- Social Security numbers
- Medical record numbers
- Photographs
- Finger and voice prints
- Diagnostic and clinical information
- Any other identifying numbers

In 2015, there was a **$5.5 million legal settlement** with one of the US's biggest healthcare systems.**

*2016 Cost of Data Breach Study: Global Analysis – Ponemon Institute, June 2016

**HHS.gov – August 2016

SOTI

The impact of BYOD on data privacy

The trend of Bring Your Own Devices (BYOD) within healthcare organizations could also be called Blame-Your-Own-Doctors. Physicians were the early-adopters that were demanding support for their personal iPhones from the IT department before proper device safeguards and data controls were even possible. Healthcare IT departments were excited by the potential of BYOD to reduce their capital expenditures on hardware and software. Healthcare workers were enthusiastic about the convenience of using their own device with its established address book and application suite. A recent study* estimated that 88% of healthcare organizations supported BYOD for their workers.

However, times have changed. Unsecured BYOD (Breach Your Own Data) devices present such a significant security and data privacy challenge, more and more healthcare organizations have discontinued support. At the same time, TCO studies are rebutting the premise that BYOD devices are cheaper at all. Any reduction in up-front costs, are eliminated by increased costs for virtualization, containerization, security and management. The healthcare market is seeing ample evidence of BYOD scepticism — within two short years the number of hospitals allowing BYOD devices decreased to 58%. More and more healthcare organizations are standardizing on COBO (corporate owned - business only) and COPE (corporate owned - personally enabled) devices.

Within 2 years, the number of healthcare organizations supporting BYOD programs has fallen by 30%.*

*SPOK's Fifth Annual Mobility Strategies in Healthcare Survey

5 simple steps to improve compliance

As important as it is to healthcare, proper mobile security goes much further than data privacy. The healthcare industry is rapidly becoming the primary target of hackers and phishers all over the globe. Healthcare organizations need to do everything they can to improve mobile security and mitigate risk.

Healthcare organizations need to do everything they can to improve mobile security and mitigate risk.

1. **Deploy an Enterprise Mobility Management (EMM) solution.** Only 41% of hospitals are using a mobility management solution*. It is impossible to properly secure and manage your organization's mobile devices without EMM.
2. **Enforce device lockdown and access code rules.** Because of their size and portability, mobile devices are prime targets for theft. At a minimum, you need to mandate device lockdown and pin-code access. You can go even further a require and complex alphanumeric passcode with a limit on retries, and a 30/60/90 data expiry period.
3. **Mandate device encryption and manage device certificates to ensure secure data transmission.** It is important to secure any data stored on the device, and data being transmitted to and from the device. Whether you are in the hospital or the neighborhood coffee shop, WiFi is inherently unsecure.
4. **Impose Data Loss Prevention (DLP) on mobile devices.** You need to make it hard for your healthcare workers to send private data outside of the hospital network. This can be done at the device level or application level. You can toggle off: cut/copy/paste, screen capture, printing and forwarding (SMS, MMS, email and chat).
5. **Use Location Services to track your devices.** Knowing the location of your mobile assets is key, but you can also employ geo-fences to restrict your mobile devices to a defined geographic area and force a lockdown (or wipe) if they leave the area.

In 2016, fourteen US based hospitals were the target of a ransomware attack and one even capitulated and paid out over $17,000 in bitcoins.**

*SPOK's Fifth Annual Mobility Strategies in Healthcare Survey

**Darkreading.com

SOTI

The IoT market will grow from an installed base of 15.4 billion devices in 2015 to **75.4 billion** in 2025.**

The Internet of Things is taking off

One of the most promising technology trends for healthcare is the Internet of Things (IoT). Research company MarketsandMarkets predicts that the healthcare IoT market will quadruple to over $160 billion by 2020. Soon there will be billions of new devices and endpoints connected together to form complex healthcare systems that run without human interaction or awareness. These new endpoints and devices will be used in hundreds of different solutions, both clinical and non-clinical.

Patient Room Controls	Motion detectors and patient data are linked to climate controls and room lighting to reduce temperature or light levels based on occupancy and patent preference.
Tracking patients, personnel and assets	Barcodes and RFID tags enable real-time location services (RTLS) for staff, patients and important assets such as wheelchairs, patient monitors, and infusion pumps as well as mobile diagnostic equipment.
Medical-grade wearable devices	New types of medical monitors and actuators can work together to create amazing healthcare solutions such as a “hybrid closed-loop insulin pump.” — commonly referred to as an artificial pancreas.***
Augmented Reality/Virtual Reality	AR and VR are powerful visualization tools that will make telemedicine easier and more accurate. Using this technology, doctors can mentor and consult over vast distances as if they were in the same operating theatre.

*MarketsandMarkets, October 2015
**IHS Technology, March 2016 - IoT platforms: enabling the Internet of Things
***Scientific American, November 2016 – The Artificial Pancreas is Here

SOTI

New technology creates new challenges

Enterprise mobility strategies, mobility management solutions and just plain experience has helped healthcare organizations to 'get good' at enterprise mobility. However just when they were getting a handle on the management needs of traditional mobile devices, the IoT is creating a new set of challenges.

New Security Challenges

As if being the primary target of most hacking, phishing and ransomware wasn't enough, the IoT is making security for healthcare much more difficult. Imagine the liability associated with a hacked pacemaker, or how a simple man-in-the-middle attack can obscure critical data from a remote glucometer and potentially lead to diabetic ketoacidosis, coma or death. Maybe this is science fiction, maybe not — but the reality is that more endpoints and more connected machines are making hacking, data breaches, and ransomware much more likely, and much more dangerous.

New Management Challenges

All the new endpoints, sensors and devices being deployed in a hospital require full lifecycle management. From a scale perspective, companies that have previously focused on dozens of COWs in the wards, and hundreds of smartphones in the hands of healthcare practitioners, will now be dealing with thousands of new devices, sensors and endpoints within their facility. These new devices are going to be incredibly diverse — beyond differences in operating system, the new endpoints will range from simple little temperature or light sensors to complex systems such as micro-manipulation robots. Keeping track of all these new devices, making sure they are up-to-date and working properly is vital for the security and success of their deployment.

A choice is no longer required

Mobile technology has created a difficult choice for healthcare organizations. On one hand, mobile devices and applications drastically improve both clinical and non-clinical workflows and help deliver superior patient care. The downside is that when left unmanaged, mobile devices are a common source of patient data leaks and an increasingly popular target for malicious activity.

Whether its MDM, EMM or UEM, mobility management eliminates the need to choose between convenience and compliance – you can have both. This is important and timely because the rapid growth of the IoT is presenting an entire new set of challenges. Healthcare organizations will need to expand the scope of their mobility management solution to deal with the new sensors, endpoints and devices of the IoT.

Mobile Device Management (MDM)	Enterprise Mobility Management (EMM)	Unified Endpoint Management (UEM)
MDM is the industry term used in the early days of enterprise mobility for the security and management of mobile devices, including: smartphones, tablets and special purpose, ruggedized devices. MDM enables rapid deployment, asset tracking, as well as device and data security features.	EMM is the term for the management of mobile devices and their applications, content, and security. It goes beyond MDM by adding management for device ownership/ deployment models, data at rest, data in transit, and wireless network connections.	UEM is the evolution of EMM in response to IoT. A UEM solution enables enterprises to secure and manage all business endpoints; from legacy mobile devices and PCs, to all the new IoT endpoints, sensors, and systems.

SOTI delivers mobility and IoT management for healthcare

SOTI has been managing mobility for more than two decades. We managed dedicated-purpose mobile devices before smartphones were introduced, and now we are leading the way to UEM and making the IoT manageable. We have a proven track record of delivering powerful, easy-to-use mobility management solutions for the healthcare industry. No matter where or how a device is used, SOTI MobiControl does it all: endpoints, applications, content, email and security are all managed from a single, unified

170+ Countries

2000+ Partners

17k+ Enterprise Customers

20+ years Experience Managing Mobility

Millions

of Devices Managed

SOTI.net

SOTI®