

# SOTI®

ONE PLATFORM  
CONNECTING EVERYTHING

## 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 in qualified personnel. This also impacts how, when and where healthcare is delivered as both patients and practitioners are opting for in-home care, either by choice or by necessity. 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

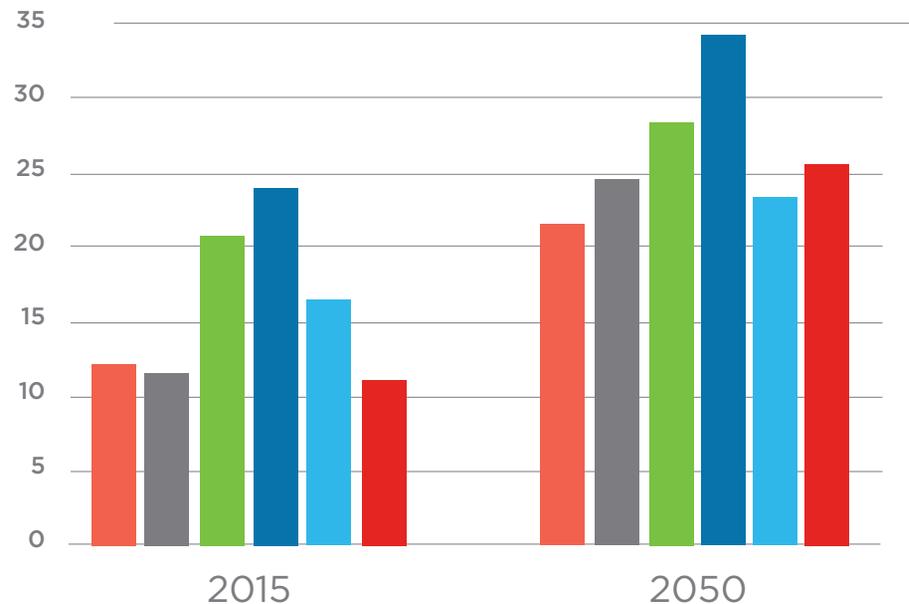
THE GLOBAL POPULATION IS GETTING OLDER	3
FEWER HEALTHCARE PRACTITIONERS AVAILABLE AND HOSPITAL SPACE ARE AT A PREMIUM	4
TOO MUCH TIME ON ADMINISTRATIVE WORK	5
HEALTHCARE ORGANIZATIONS ARE EMBRACING MOBILE TECHNOLOGY	6
HOW ARE HEALTHCARE WORKERS USING MOBILE TECHNOLOGY?	7
NON-CLINICAL DEVICES AND APPLICATIONS STREAMLINE OPERATIONS	8
PATIENT DATA PRIVACY AROUND THE WORLD	9
HOW COMMON ARE HEALTHCARE DATA BREACHES?	10
COMMON THREATS TO HEALTHCARE DATA PRIVACY	11
THE CONSEQUENCES OF DATA PRIVACY BREACHES	12
THE IMPACT OF BYOD ON DATA PRIVACY	13
5 SIMPLE STEPS TO IMPROVE COMPLIANCE	14
THE INTERNET OF THINGS HAS TAKEN OFF	15
NEW TECHNOLOGY CREATES NEW CHALLENGES	16
A CHOICE IS NO LONGER REQUIRED	17
SOTI DELIVERS MOBILITY AND IoT MANAGEMENT FOR HEALTHCARE	18

# THE GLOBAL POPULATION IS GETTING OLDER

Declining fertility and increasing longevity are rapidly aging the world's population. The World Health Organization (WHO) predicts that by 2050, 22% of the world's population will be aged 60 and over.<sup>1</sup> Also by 2050, over 430 million people worldwide will be aged 80 and over.<sup>2</sup>

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 healthcare.

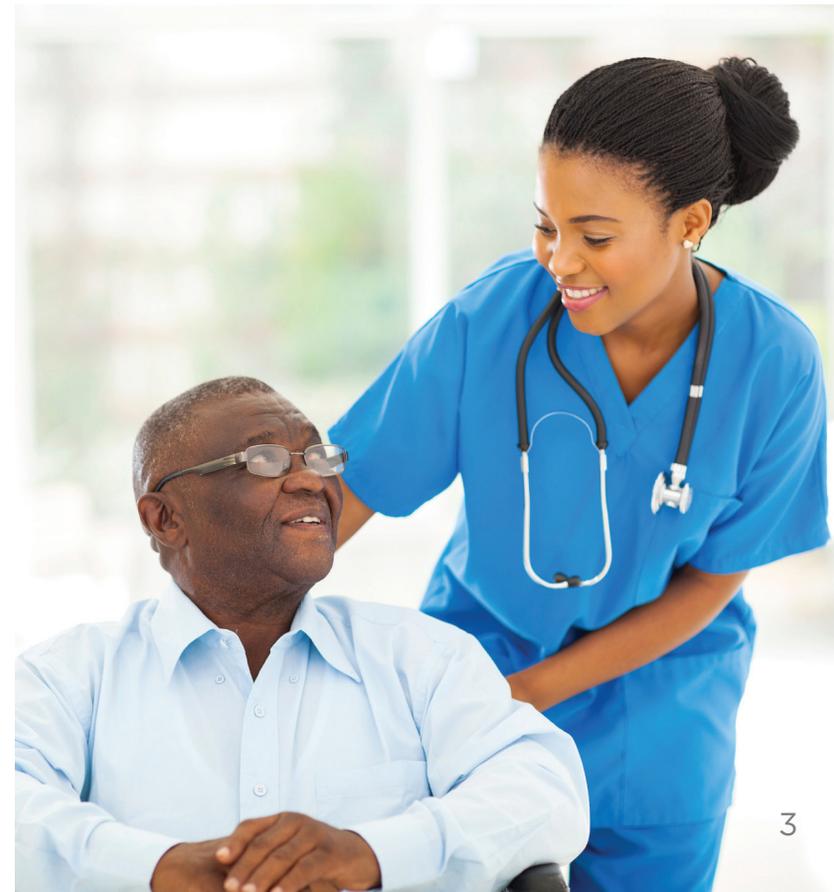
## % OF POPULATION AGED 60 YEARS OR OLDER BY REGION



● World ● Asia ● North America ● Europe ● Oceania ● Latin America

1. WHO, Aging and Health, 2018

2. WHO, Aging and Health, 2018



# FEWER HEALTHCARE PRACTITIONERS ARE AVAILABLE AND HOSPITAL SPACES ARE AT A PREMIUM

Just as the demand for healthcare is ramping up, many countries and their healthcare systems are experiencing a shortage in physicians, nurses, allied health professionals and overall hospital spaces. The World Health Organization (WHO) forecasts a global deficit of almost 13 million trained health professionals by 2035.<sup>3</sup> 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.<sup>4</sup>
- In 2019, the National Health Service (NHS) in the UK estimated there were 43,617 nursing vacancies. That's an increase of approximately 86% compared to 2016.<sup>5</sup>
- India has over 400 medical schools, but still has a shortfall of over 750,000 doctors.<sup>6</sup>

3. World Health Organization, 2013- A Universal Truth - No Health without a Workforce

4. American Association of Medical Colleges (AAMC)

5. Nursing Times, NHS Nurse Vacancies in England Rise to More than 43,000

6. N World, Shortage of Doctors in India Takes a Toll on Public Health



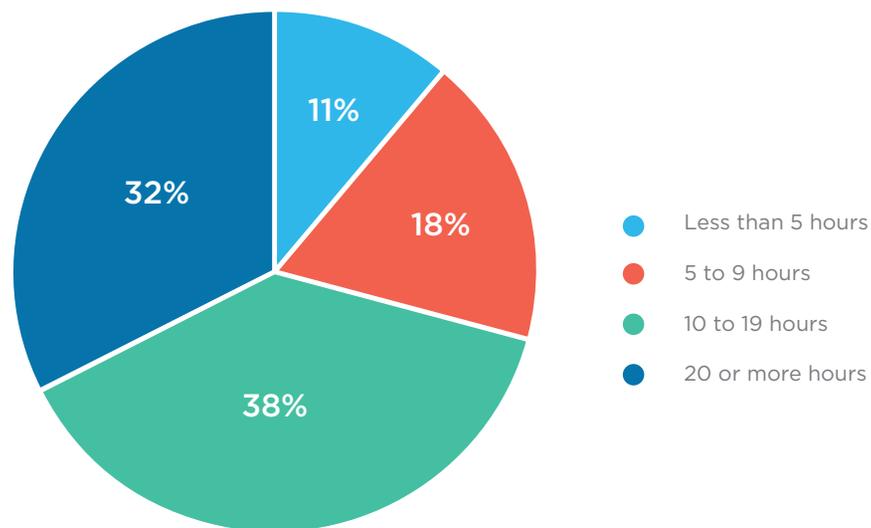
**THE WORLD  
WILL BE SHORT  
12.9 MILLION  
HEALTHCARE  
WORKERS  
BY 2035.<sup>3</sup>**

# TOO MUCH TIME SPENT ON ADMINISTRATIVE WORK

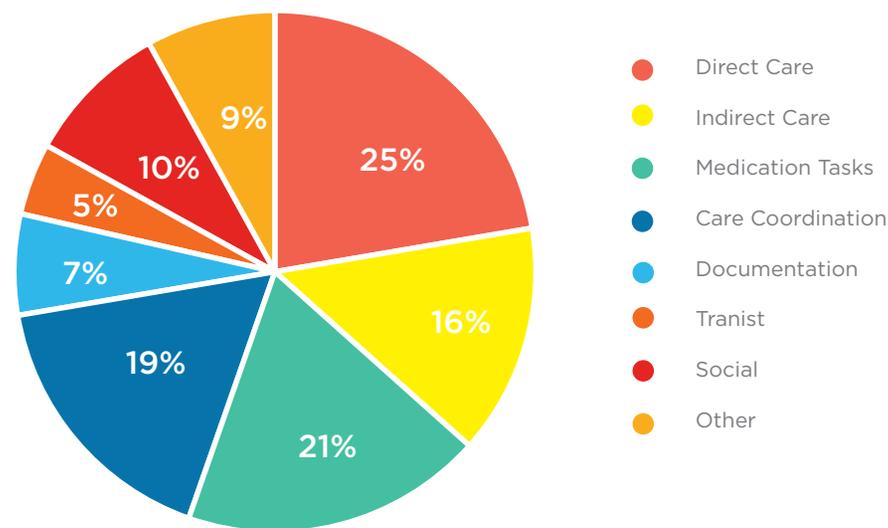
Hospitals are deploying Healthcare Information Systems (HIS) to improve clinical workflows and reduce potentially lethal medical errors. Even so, physicians and nurses are spending more and more of their day dealing with administrative duties and non-clinical activities. A recent, multi-specialty time and motion study found that 70% of physicians spend 10 hours or more weekly on paperwork or administrative tasks. The same report shows that only 14% of physicians spend 30 hours or more seeing patients.<sup>7</sup> 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.<sup>8</sup>

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 ON PAPER AND ADMINISTRATION



NURSE TIME DISTRIBUTION



7. AMA, Do You Spend More Time on Administrative Tasks than Your Peers?

8. 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

# 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 USD in 2015 to almost \$150 billion USD by 2023.<sup>9</sup> 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.<sup>10</sup> 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, Wi-Fi phones, tablet computers, voice badges and wearables.



**90% OF HEALTHCARE PRACTITIONERS ARE USING MOBILE DEVICES TO ENGAGE PATIENTS DIRECTLY, AT THE POINT OF CARE.<sup>11</sup>**

9. 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

10. SPOK's Fifth Annual Mobility Strategies in Healthcare Survey

11. 2015 HIMSS Mobile Technology Survey

# HOW ARE HEALTHCARE WORKERS USING MOBILE TECHNOLOGY?

Approximately 80% of physicians are willing to use their personal device within the workplace in a Bring Your Own Device (BYOD) manner in order to support their work.<sup>12</sup>

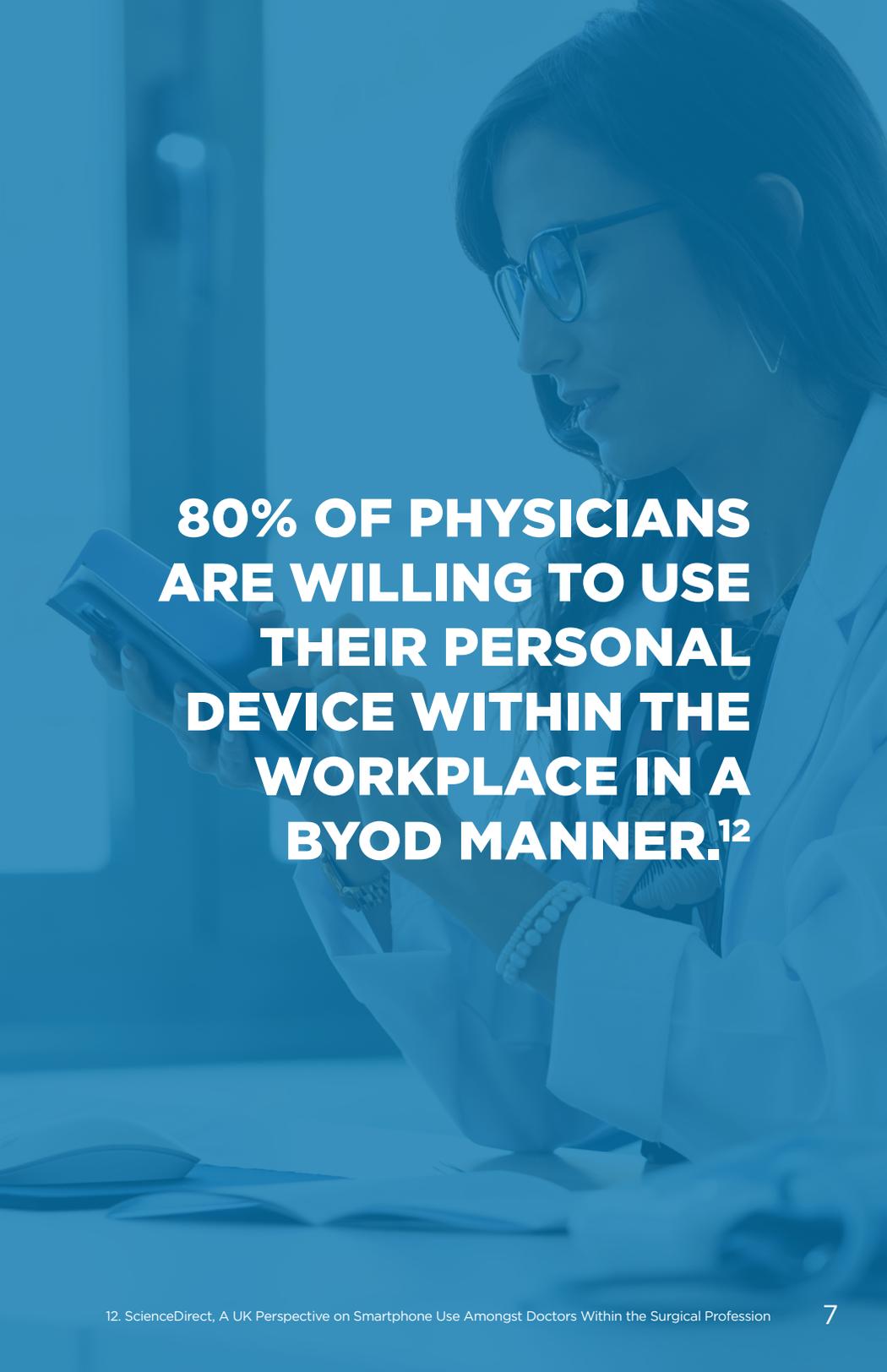
Healthcare workers are using mobile devices for:

- Communication and Collaboration – Voice, video conferencing, text and email.
- Accessing Healthcare Information Systems – Electronic health/medical records (EHR and 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 ARE WILLING TO USE THEIR PERSONAL DEVICE WITHIN THE WORKPLACE IN A BYOD MANNER.<sup>12</sup>**



# 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:

<b>Self-Registration Kiosks</b>	Tablets and touchscreen computers reduce staff workload, makes the patient registration process faster and reduces data errors.
<b>Logistics for Porters</b>	Remotely allocate tasks to porters based on location, priority and current workload. This reduces delays, improves porter utilization, and provides improved visibility and reporting.
<b>Appointment Scheduling</b>	Mobile applications makes it easier for patients to schedule appointments with physicians, therapists and medical services. <sup>13</sup>
<b>Wayfinding/Navigation</b>	Mobile applications and kiosk technology help patients and their families navigate around the hospital and locate points of interest such as ATMs, gift shops and food courts. <sup>14</sup>
<b>Hospital Maintenance</b>	Computerized maintenance management system (CMMS) schedules, assigns and tracks maintenance work orders.

13. San Diego Tribune - November 9, 2016 - VA to launch online appointment scheduling

14. 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 USA 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. Below are five regions who have spearheaded the passing of legislation designed to protect confidential patient 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.

- In 2019, 67% of UK healthcare organizations experienced a cyberattack. The majority of those attacks originated from viruses or malware introduced on third-party devices.<sup>15</sup>
- It's estimated that the loss of data and related failures will cost healthcare companies \$6 trillion in damages in 2020 alone. Because of this, 82% of healthcare organizations agree that digital security is one of their foremost concerns.<sup>16</sup>
- 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.<sup>17</sup>

**75% OF  
HEALTHCARE  
ORGANIZATIONS  
GLOBALLY HAVE  
EXPERIENCED  
CYBERATTACKS.<sup>18</sup>**

15. ComputerWeekly.com, Two-thirds of UK Healthcare Organizations Breached Last Year

16. PhoenixNAP, Healthcare Data Breaches, By the Numbers

17. ITNews, Australia's Biggest Data Breach Sees 1.3m Records Leaked

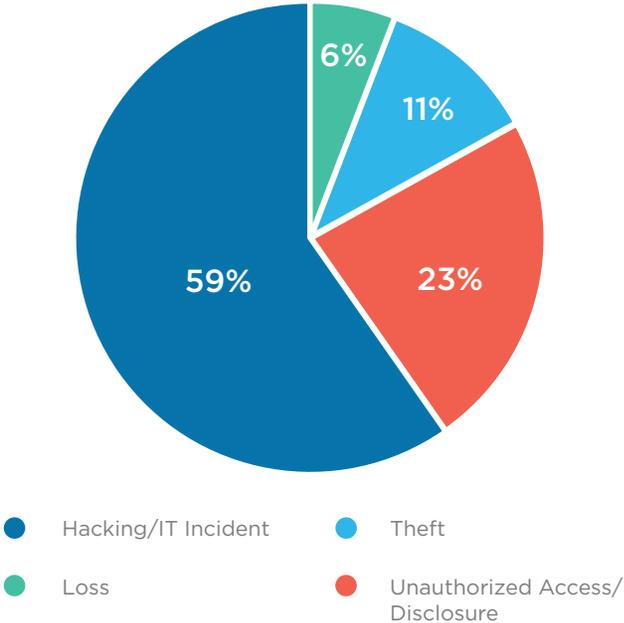
18. Security Magazine, 75% of Healthcare Organizations Globally Have Experienced Cyberattacks

# 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:

<p><b>Improper Use/Disposal</b></p>	<p>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, organizations need to be careful how their employees are handling patient records – how and where they are accessed, filed and archived.</p>
<p><b>Unauthorized Access/Disclosure</b></p>	<p>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.</p>
<p><b>Theft</b></p>	<p>As enterprise mobile devices have shrunk in size and grown in capabilities, they are increasingly the target of theft. When you consider that as many as 14% of doctor devices are completely unsecured<sup>19</sup>, it is an easy way for criminals to access patient data, or even the hospitals secure HIS systems.</p>
<p><b>Loss</b></p>	<p>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.</p>
<p><b>Hacking/IT Incident</b></p>	<p>Increasingly, healthcare systems are being targeted by cybercriminals to either steal patient data, or lockdown the system and extract payment, commonly called Ransomware.</p>

**TOP CAUSES OF HEALTHCARE DATA BREACHES ON 2019<sup>20</sup>**



19. DarkReading, April 2016 – Doctors’ MobileDevices Putting Patient at Risk  
 20. HIPAA Journal, 2019 Healthcare Data Breach Report

# 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. Data breaches in the healthcare industry are the most expensive at approximately \$429 per patient globally.<sup>21</sup> Based on breach size and frequency, the average total cost of a data breach increased to \$6.5 million.<sup>22</sup>

## 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

21. Health IT Security, Data Breaches Cost Healthcare \$6.5M, or \$429 Per Patient Record

22. Health IT Security, Data Breaches Cost Healthcare \$6.5M, or \$429 Per Patient Record

23. PhoenixNAP, Healthcare Data Breaches, By the Numbers



**IN 2017, U.S. HEALTHCARE COMPANIES COLLECTIVELY LOST \$3 TRILLION DUE TO DATA LOSS.<sup>23</sup>**

# THE IMPACT OF BYOD ON DATA PRIVACY

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 estimates that although 68% of healthcare organizations have some form of BYOD policy, only 39% have a mobile data management system in place.<sup>24</sup>

However, times have changed. Unsecured BYOD devices present such a significant security and data privacy challenge, more and more healthcare organizations have discontinued support. 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 as the BYOD movement has struggled to gain traction in healthcare. More and more healthcare organizations are standardizing on Corporately Owned, Business Only (COBO) and Corporately Owned, Personally Enabled (COPE) deployment scenarios.



**WHILE 68% OF HEALTHCARE ORGANIZATIONS HAVE A BYOD POLICY, ONLY 38% HAVE A MOBILE DATA MANAGEMENT SYSTEM IN PLACE.<sup>25</sup>**

24. Beckers Hospital Review, 9 Statistics on BYOD Security Policies

25. Becker's Health IT, 9 Statistics on BYOD Security Policies

# 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.

1. **Deploy an Enterprise Mobility Management (EMM) solution.** Only 41% of hospitals are using a mobility management solution.<sup>26</sup> It is impossible to properly secure and manage your organization's mobile devices without an EMM solution.
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 and require a 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 neighbourhood coffee shop, Wi-Fi 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 geofences to restrict your mobile devices to a defined geographic area and force a lockdown (or wipe) if they leave the area.

26. SPOK's Fifth Annual Mobility Strategies in Healthcare Survey  
27. Darkreading.com

**IN 2016, 14 U.S. BASED HOSPITALS WERE THE TARGET OF A RANSOMWARE ATTACK AND ONE EVEN CAPITULATED AND PAID OUT OVER \$17,000 IN BITCOINS.<sup>27</sup>**

# THE INTERNET OF THINGS HAS TAKEN OFF

One of the most exciting technology trends for healthcare is the Internet of Things (IoT). It's expected that the IoT in healthcare market will be worth over \$534 billion USD by 2025.<sup>28</sup> 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 patient preference.
Tracking Patients, Personnel & Assets	Barcodes and RFID tags enable real-time location services (RTLS) for staff, patients and important assets such as: wheelchairs, patient monitors, infusion pumps and 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. <sup>30</sup>
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 room.

**THE IoT MARKET WILL GROW FROM AN INSTALLED BASE OF 15.4 BILLION DEVICES IN 2015 TO 75.4 BILLION IN 2025.<sup>29</sup>**

28. Grand View Research, IoT in Healthcare Market Worth \$534.3 billion by 2025

29. IHS Technology, March 2016 - IoT platforms: enabling the Internet of Things

30. Scientific American, November 2016 - The Artificial Pancreas is Here

# 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 (MITM) 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 Computers on Wheels (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.

Enterprise Mobility Management (EMM) 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.

## Enterprise Mobility Management (EMM)

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.



# SOTI DELIVERS MOBILITY AND IoT MANAGEMENT FOR HEALTHCARE

Advancements in mobile device capabilities and healthcare organizations' technical infrastructure, have enabled medical practitioners to deploy devices to securely collect patient data, update patient records and assist in valuable research for gaining deeper insights into collected data. But more mobile devices and apps means an increase in management complexity, including: security, remote support, app and content distribution, privacy and mobile device analytics. SOTI helps healthcare organizations manage critical technology for critical care.

**170+** COUNTRIES

**2,000+** PARTNERS

**17K+** ENTERPRISE CUSTOMERS

**20+ YEARS** EXPERIENCE MANAGING MOBILITY



**MILLIONS**  
OF DEVICES MANAGED

## TO LEARN MORE:

For additional information on how SOTI provides critical technology for critical care, visit [soti.net/healthcare](https://soti.net/healthcare).

To learn more about the SOTI ONE Platform, visit [soti.net/one](https://soti.net/one).

You can also contact us anytime with your questions, or arrange a free demo at [soti.net/about/contact-us](https://soti.net/about/contact-us).

SOTI is a proven innovator and industry leader for simplifying business mobility and IoT solutions by making them smarter, faster and more reliable. SOTI helps businesses around the world take mobility to endless possibilities.

[soti.net](https://soti.net)