BYOD TRENDS IN HEALTHCARE: AN INDUSTRY SNAPSHOT
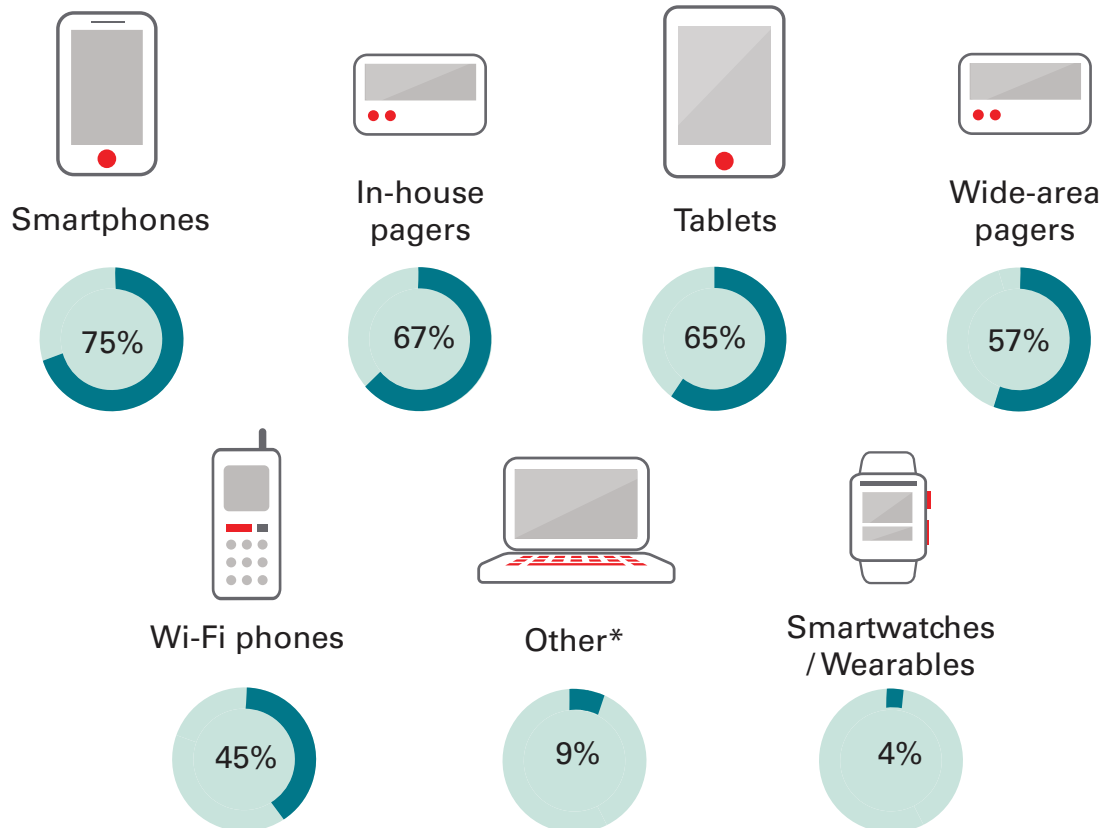
2015 SURVEY RESULTS REVEALED

HOW DO YOU BYOD?

A popular topic for hospitals right now is whether to allow employees to use their personal smartphones and tablets for staff communications and patient alerts. "Bring your own device" (BYOD) is a challenging issue because it encompasses so many questions related to an organization's costs, security risks, IT availability, and the varying needs of different groups of staff. There is no one-size-fits all answer, and the landscape is changing rapidly as mobile strategies in healthcare mature.

In June 2015, Spok surveyed more than 450 healthcare organizations for a snapshot of the current state of BYOD. Survey participants were from hospitals of all sizes across North America and included leaders in the executive suite, IT and telecommunications departments, as well as clinical and administrative staff. Evolving staff workflows, different facility infrastructures, and unequal risk tolerance mean that there is still a lot of variation across the industry.

WHICH TYPES OF MOBILE DEVICES DOES YOUR ORGANIZATION SUPPORT?

Smartphones
75%

In-house pagers
67%

Tablets
65%

Wide-area pagers
57%

Wi-Fi phones
45%

Other*
9%

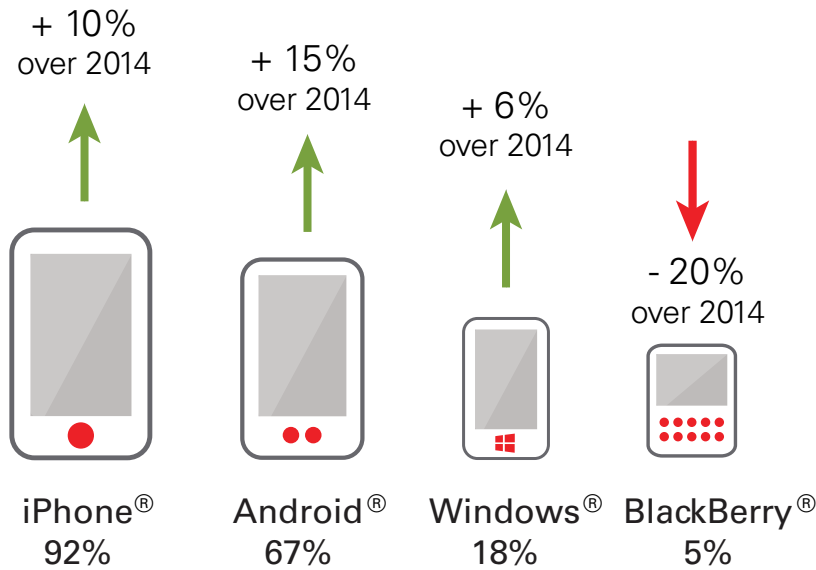**Smartwatches / Wearables**
4%

Key take-away: Clinician preferences, workflow optimization, and differing needs across hospital roles are keeping the mobile device mix diverse. A communications platform with the ability to coordinate messages to all of these devices is essential to fully support mobile workflows.

Note: Tablet support is up 12 percent over 2014. This is likely driven by residency programs, as well as a shifting user preferences as clinicians and others move away from laptops to these smaller, lighter devices.

*Many of the survey respondents who stated "other" indicated staff use voice badges, radios and laptops

WHAT TYPES OF SMARTPHONES DOES YOUR ORGANIZATION SUPPORT?

+ 10% over 2014

+ 15% over 2014

+ 6% over 2014

- 20% over 2014

iPhone®
92%

Android®
67%

Windows®
18%

BlackBerry®
5%

Of the smartphones and tablets in use today at your hospital for work-related purposes, what percentage of these devices are personal? What percentage are hospital-issued?

48% Personal (down 7%)

52% Hospital-issued (up 7%)

DOES YOUR ORGANIZATION CURRENTLY ALLOW SOME FORM OF BRING YOUR OWN DEVICE (BYOD)?

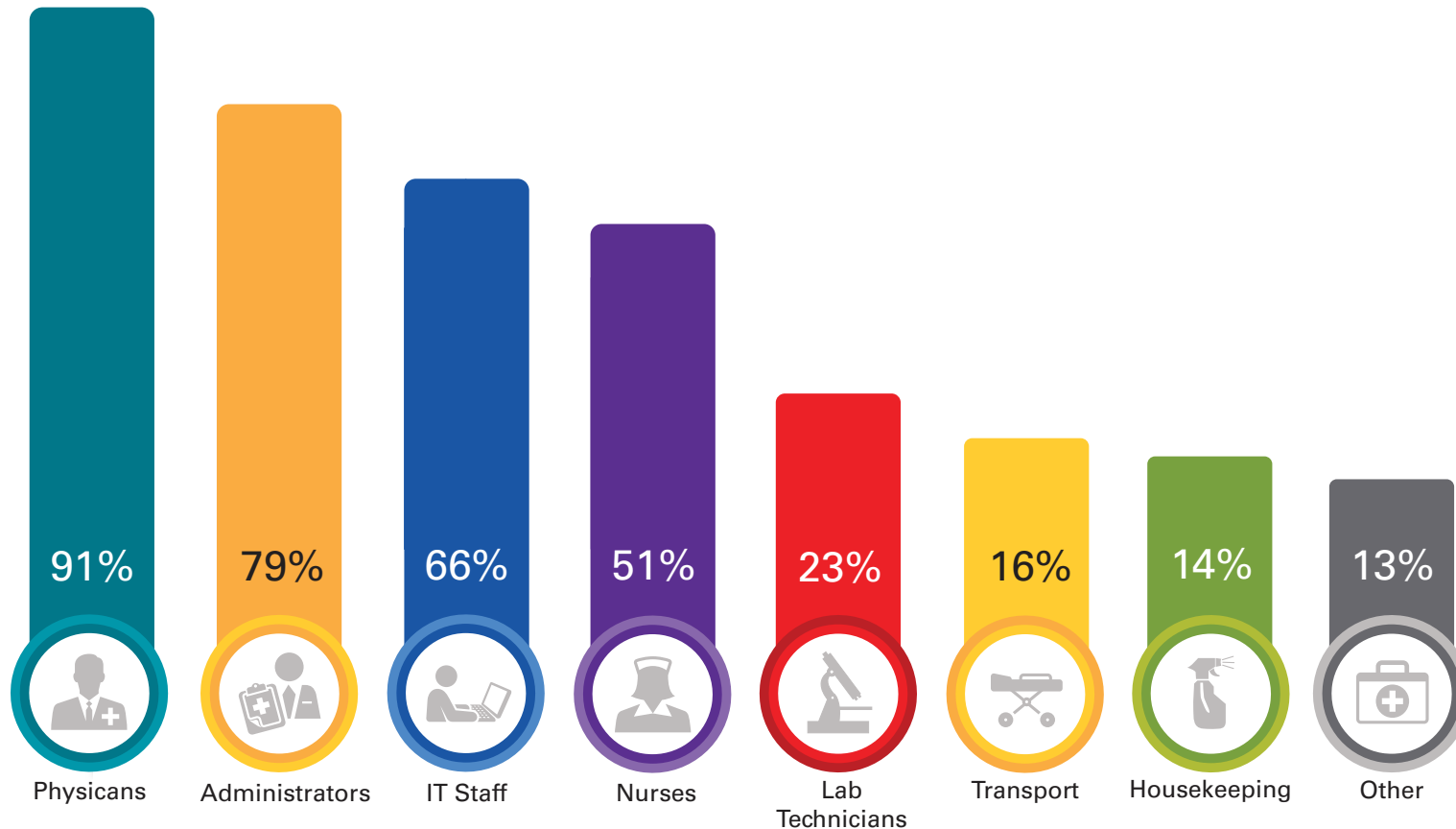**73% Yes** (2014 = 88%)

27% No (2014 = 12%)

There appears to be a moderate shift away from allowing BYOD. In 2014, 88 percent of respondents indicated that their facility allowed some form of BYOD, compared to only 73 percent this year. The overall mix of personal versus hospital-issued devices is also changing, and we're seeing a decrease of BYOD usage in favor of hospital-issued devices. This is in contrast to Gartner research[1] which predicts that 90 percent of organizations will support some aspect of BYOD by 2017, and that by 2018 there will be twice as many employee-owned devices in the workplace as enterprise-owned devices. We think there are two major distinctions that contribute to this disconnect between predicted growth in BYOD and the actual reported decline. First, healthcare is a special industry because of patient privacy laws, and second, different roles within a hospital may be best served by devices other than consumer-grade smartphones and tablets.

Exploring the first idea, that healthcare's patient privacy laws require special consideration, data security was the most commonly cited challenge within BYOD environments (62 percent), as well as the most frequently cited reason for prohibiting BYOD altogether (81 percent). Given the delicacy of handling patients' protected information, it is not surprising that more institutions are simply removing personal devices from the mobile mix as a way to retain more control over data and protect patients and hospitals from additional risk for data breaches.

[1]http://www.networkworld.com/article/2854044/microsoft-subnet/byod-is-saving-serious-money-for-it
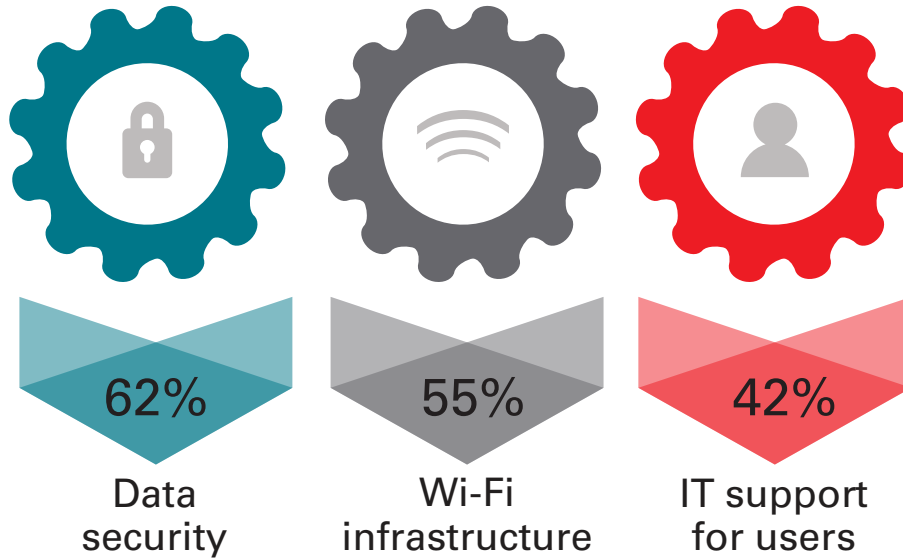
WHAT STAFF MEMBERS ARE ALLOWED TO PARTICIPATE IN THE BYOD PROGRAM?

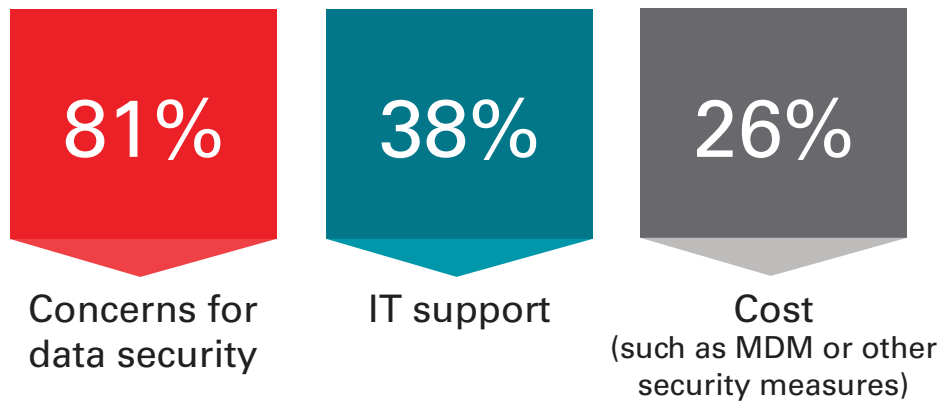| Physicians	Administrators	IT Staff	Nurses	Lab Technicians	Transport	Housekeeping	Other
91%	79%	66%	51%	23%	16%	14%	13%

The second contributing factor relates to the variation in hospital workflows across different roles. Within hospitals that indicated they do allow some form of BYOD, permission to use personal devices is unequally distributed among staff: 91 percent support BYOD for physicians and 79 percent for administrators, but only 51 percent for nursing staff. Part of this difference could be because 38 percent of respondents cited physician demand as one of the main drivers for pursuing a BYOD environment in the first place.

Another driver could be the contrast between physician and nursing roles and their differing communication needs. Nurses need to communicate largely during their shift while physicians often field patient-specific questions when on call, during non-rounding hours, and when traveling between locations. In addition, we've learned through numerous customer conversations that more hospitals are purchasing devices for nursing staff. This is because shared devices are easier to secure, support more specialized healthcare functionality, are more durable, and can be more cost effective.
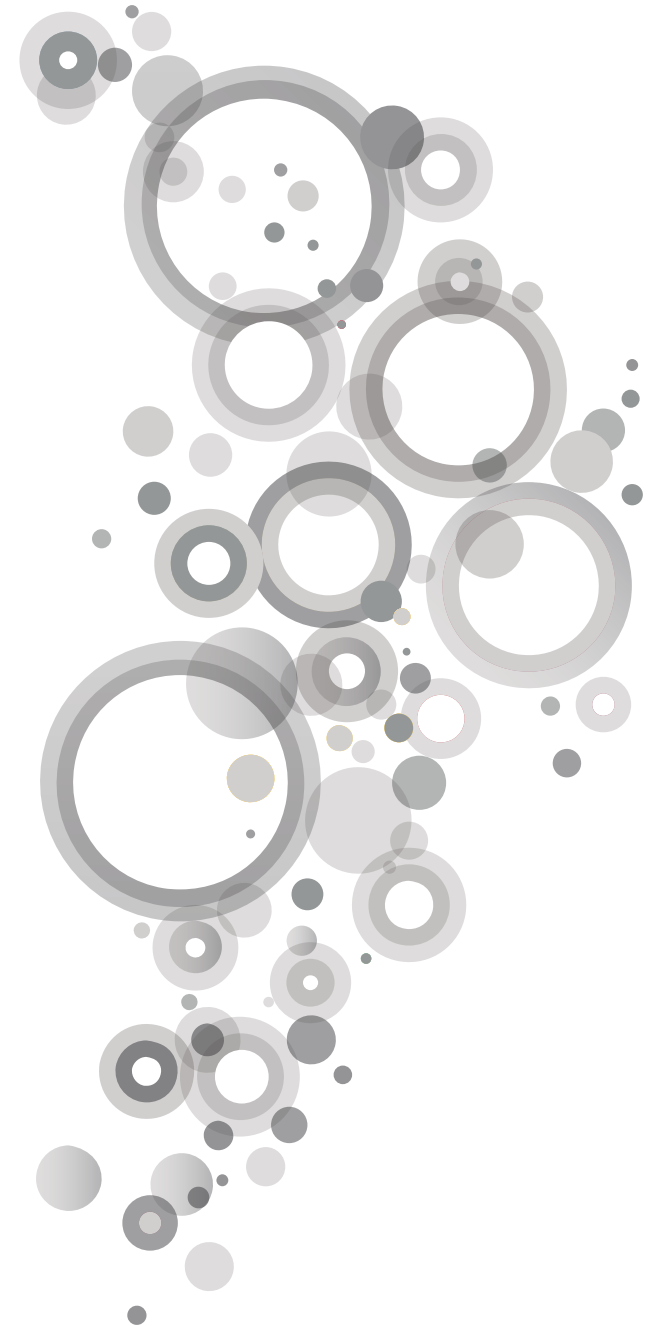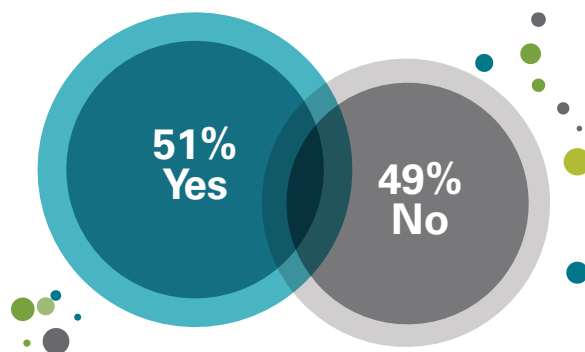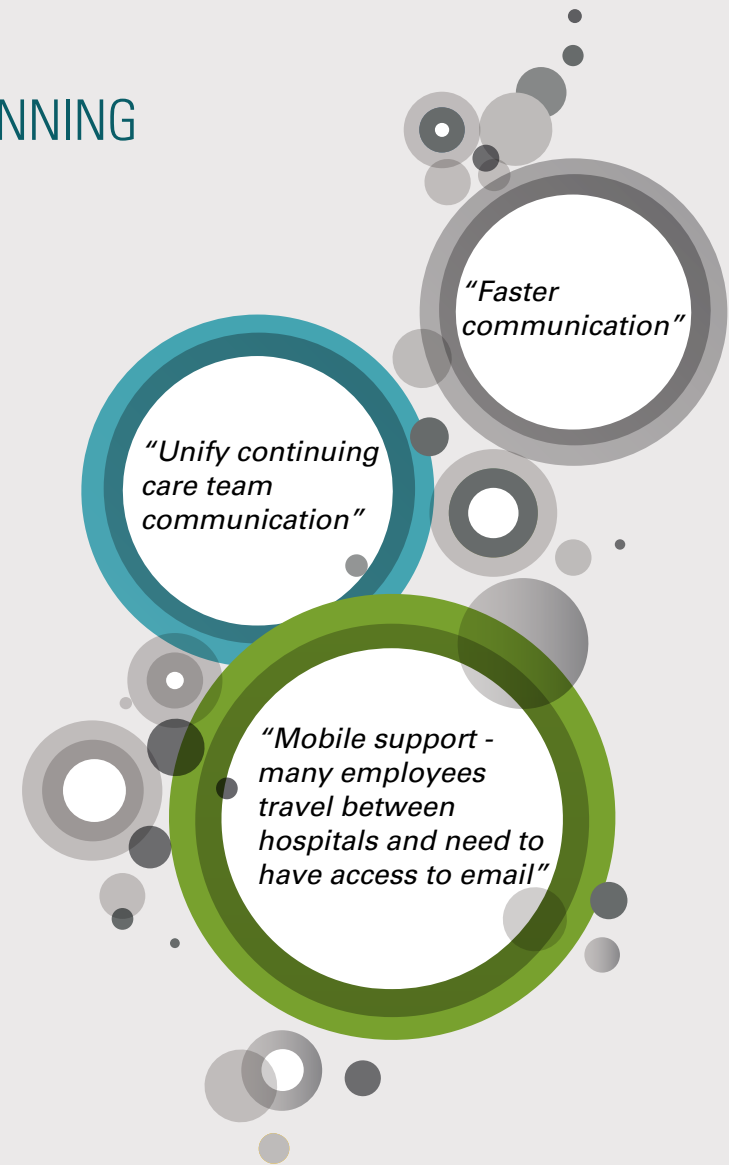
TOP THREE BYOD CHALLENGES:
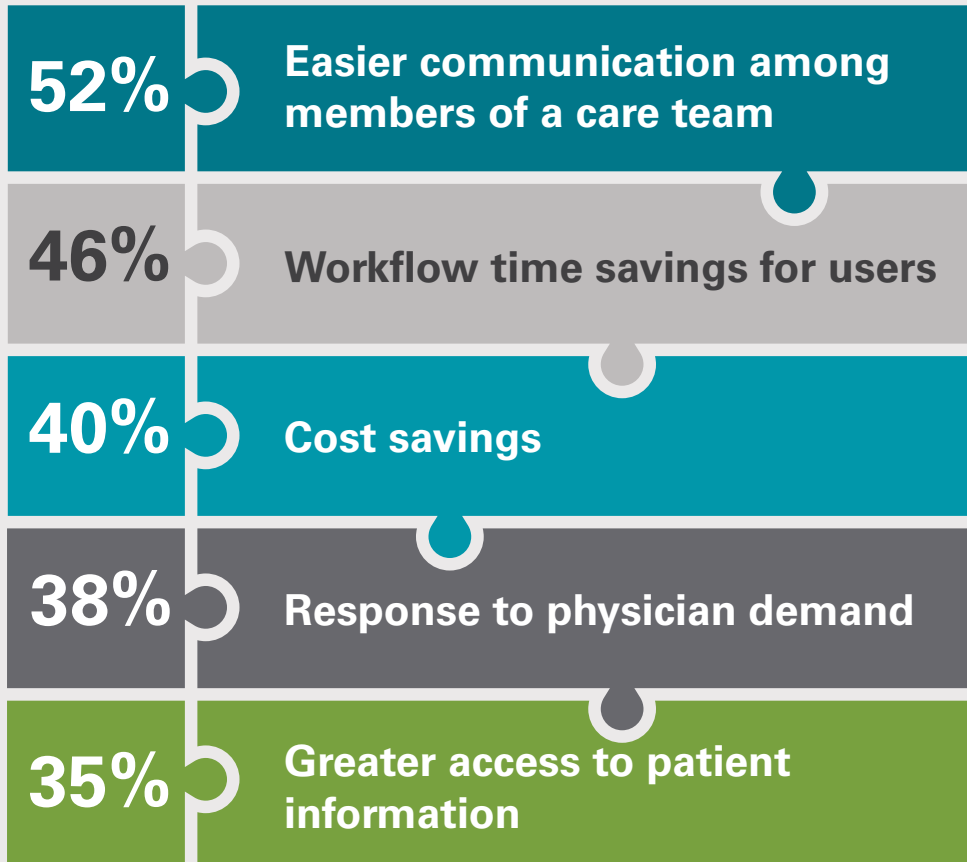
62% — Data security

55% — Wi-Fi infrastructure

42% — IT support for users

PRIMARY REASONS FOR NOT ALLOWING BYOD:

81% — Concerns for data security

38% — IT support

26% — Cost (such as MDM or other security measures)

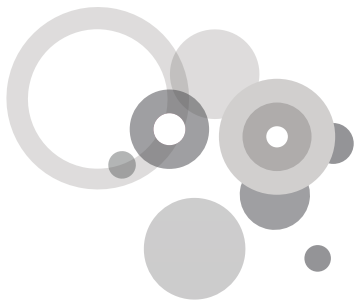*"Device might be used for personal entertainment during work hours"*

TOP FIVE DRIVERS FOR ALLOWING OR CURRENTLY PLANNING FOR A BYOD ENVIRONMENT:

52% Easier communication among members of a care team

46% Workflow time savings for users

40% Cost savings

38% Response to physician demand

35% Greater access to patient information

"Faster communication"

"Unify continuing care team communication"

"Mobile support - many employees travel between hospitals and need to have access to email"

51% Yes

49% No

DOES YOUR ORGANIZATION HAVE A DEFINED BYOD POLICY?

Of the organizations that allow some form of BYOD there is nearly an even split between hospitals with and without a defined BYOD policy.
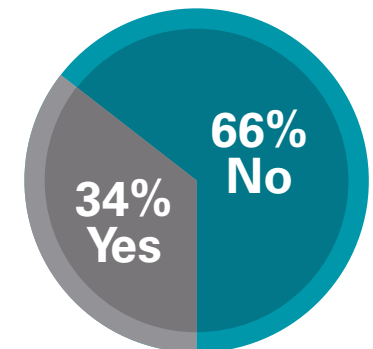
TOP FOUR AREAS BYOD POLICIES COVER :

Device Security

89%

Enforcement for non-compliance with policy

74%

What device types are supported

72%

Who pays for cellular and data plans

65%
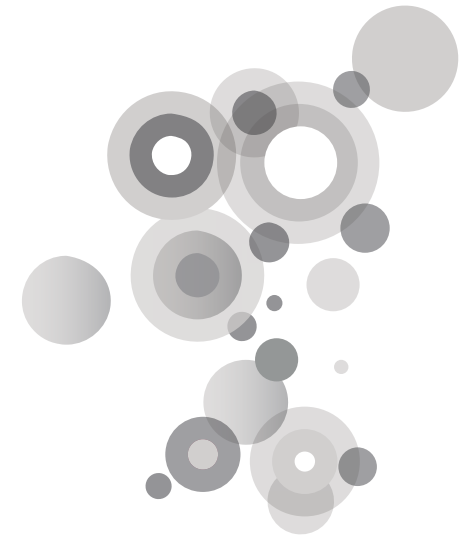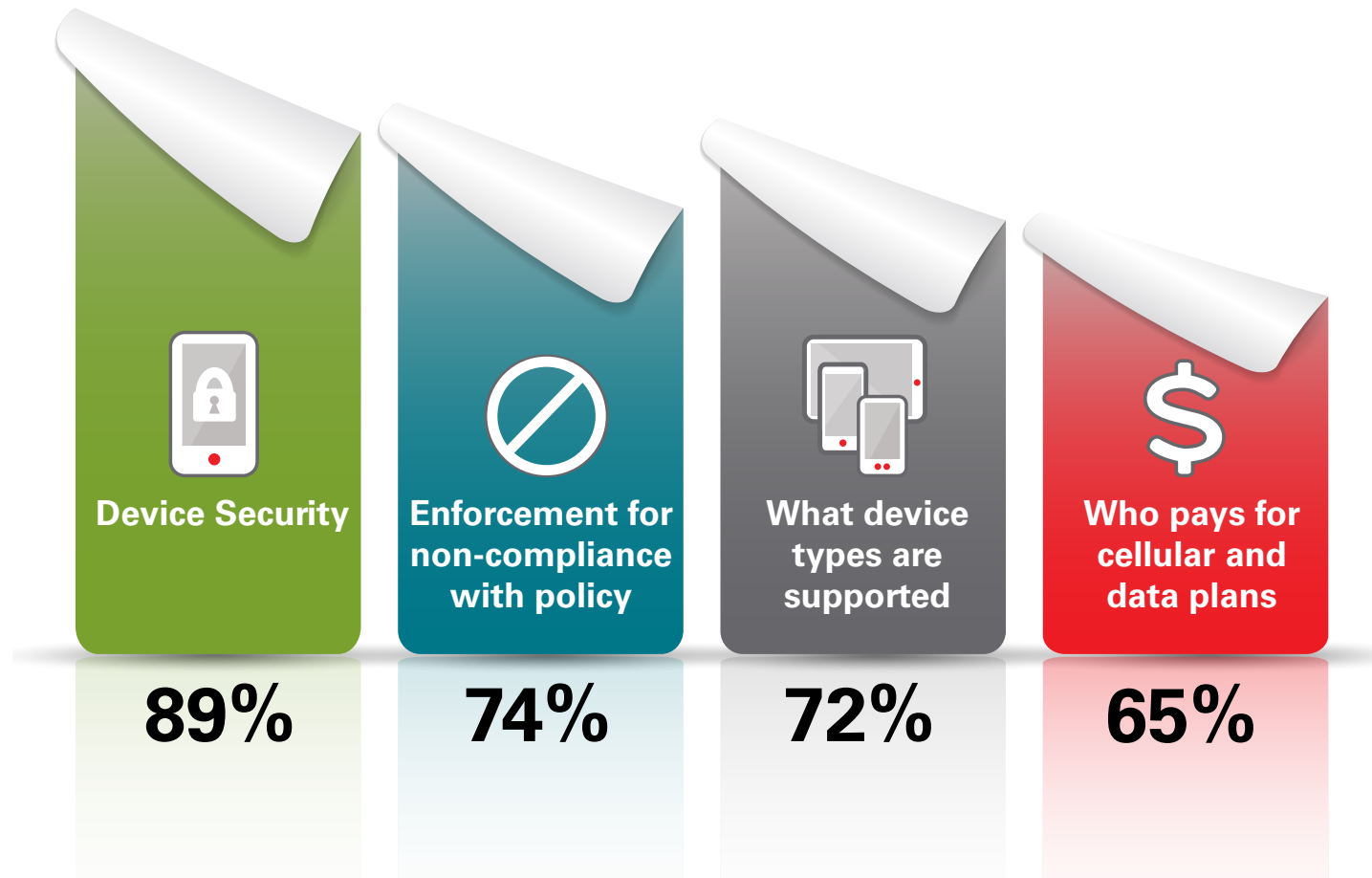
IF YOUR HOSPITAL DOES NOT CURRENTLY ALLOW BYOD, IS THIS A FUTURE INITIATIVE?

66% No

34% Yes

WHO WAS OR WILL BE INVOLVED IN CREATING AN OVERALL MOBILITY STRATEGY FOR YOUR HOSPITAL?

78%
IT department

43%
Clinical leadership

32%
Telecom department

28%
Doctors

With security persisting as the largest concern for BYOD (both within existing BYOD environments and as a compelling reason not to allow them), it is surprising that only 47 percent of all hospitals surveyed currently provide their users with a secure texting solution. Of those who have deployed a secure texting app, the majority indicated securing protected health information (PHI) as a primary driver for use (78 percent), followed by the need to support easier physician-to-physician conversations (59 percent). We further examined our data and did find that secure texting is more prevalent in BYOD versus non-BYOD settings, but only by 4 percent. We also expected to see a larger number of institutions using a mobile device management (MDM) solution to help manage security, but progress in this area remains largely unchanged from last year.
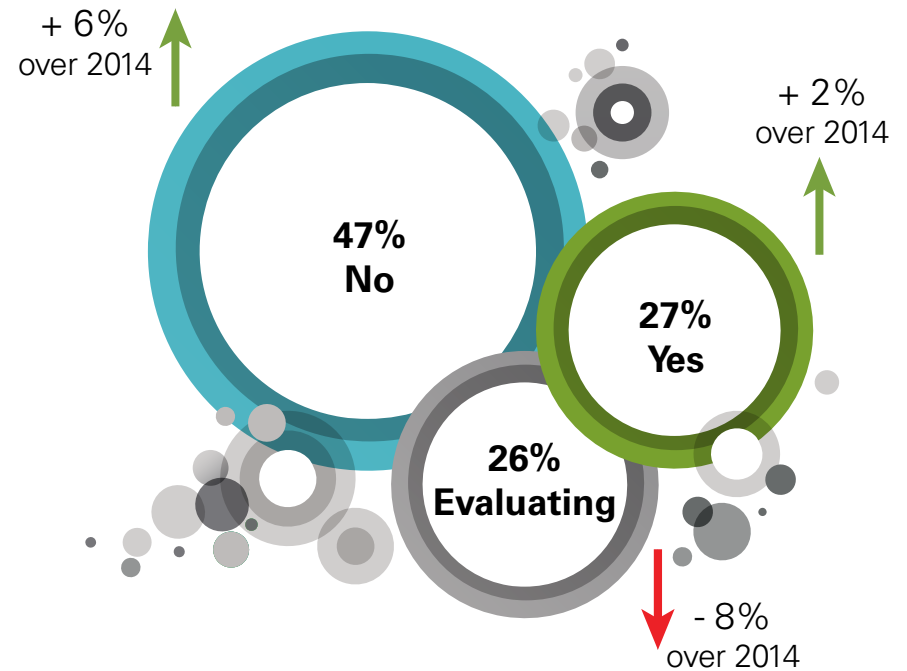
DOES YOUR HOSPITAL USE A SECURE TEXTING SOLUTION?

47%
Yes

53%
No
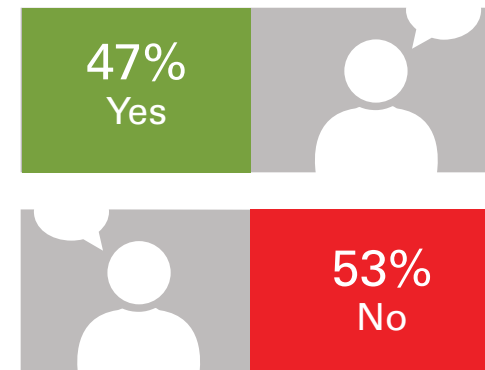
SECURE TEXTING BY ENVIRONMENT

Non BYOD
56% No   44% Yes

BYOD
52% No   48% Yes

TOP FOUR DRIVERS FOR DEPLOYING A SECURE TEXTING SOLUTION:

- Maintain security of protected health information (PHI) — **78%**
- Support easier physician-to-physician conversations — **59%**
- Care team communication / coordination of care — **52%**
- Ability to send staff messages (code calls, transport assignments, nurse-call requests, etc.) — **52%**

DOES YOUR HOSPITAL USE A MOBILE DEVICE MANAGEMENT (MDM) SOLUTION?

47% No — + 6% over 2014

27% Yes — + 2% over 2014

26% Evaluating — - 8% over 2014

SUMMARY

Discussions about mobile healthcare workflows continue. More efficient communication among care team members, and time/cost savings remain top drivers for pursuing a BYOD environment, and information security continues to be a key concern. Yet only 47 percent of hospitals reported using a secure texting solution, and 27 percent said they use a mobile device management (MDM) solution. Contrasting with the expressed concerns for data and device security, growth in these areas may be slow because of competing priorities for IT attention and budget, as well as the shifting focus we are hearing through conversations with customers.

Hospitals are now thinking more broadly than just whether to allow BYOD, offer secure texting, or use MDMs. Looking to the future, leaders are seeking broader solutions to facilitate better transfer of information for comprehensive workflow improvements and optimal patient care throughout the hospital facility. BYOD is a small piece of a much larger puzzle that is taking time for many institutions to frame and fill in the pieces. It will be interesting to watch the picture come into focus as mobile technologies advance, communication solutions evolve, and more and more hospitals set mobility preferences that support their clinical workflows and patient care initiatives.
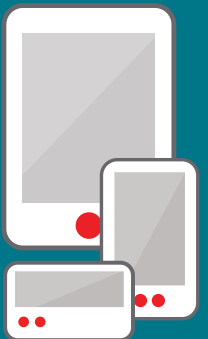
ABOUT SPOK, INC.

Spok, Inc., a wholly owned subsidiary of Spok Holdings, Inc. (NASDAQ: SPOK), headquartered in Springfield, Va., is proud to be a leader in critical communications for healthcare, government, public safety, and other industries. We deliver smart, reliable solutions to help protect the health, well-being, and safety of people around the globe. Organizations worldwide rely on Spok for workflow improvement, secure texting, paging services, contact center optimization, and public safety response. When communications matter, Spok delivers.

spok.com

/ Spoktweets