



# IT Trends in Health Care: A Survey Report

Bob O'Donnell, Founder and Chief Analyst



# Agenda

- Study Purpose
- Methodology
- Summary Results
- Conclusions
- Complete Survey Results



# Study Purpose

- The goal of this study was to understand important trends impacting IT in US health care organizations of all sizes
- The study specifically looked into:
  - Device Purchase and Usage Trends
  - BYOD Adoption
  - Desktop Virtualization
  - Security and Authentication
  - Custom Application Development
  - Infrastructure
  - Consumer Wearables (Health and Fitness)



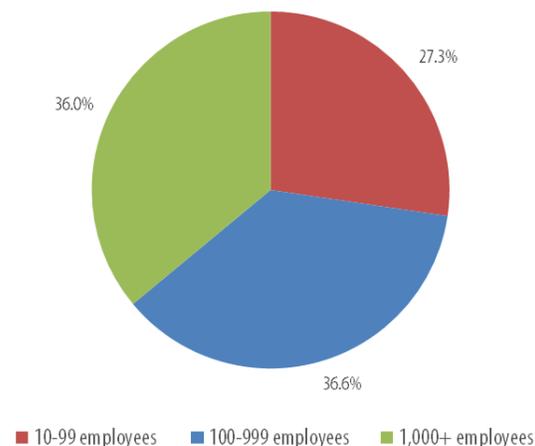
# Methodology

- The study was conducted during May and June 2015 via an online survey of 322 IT professionals employed in the health care industry
- Respondents needed to be responsible for the purchase and/or management of client devices (such as PCs, tablets, smartphones) or infrastructure (such as servers, storage, networking)
- Respondents came from a mix of:
  - Small organizations (10-99 employees)
  - Medium organizations (100-999 employees)
  - Large organizations (1,000+ employees)

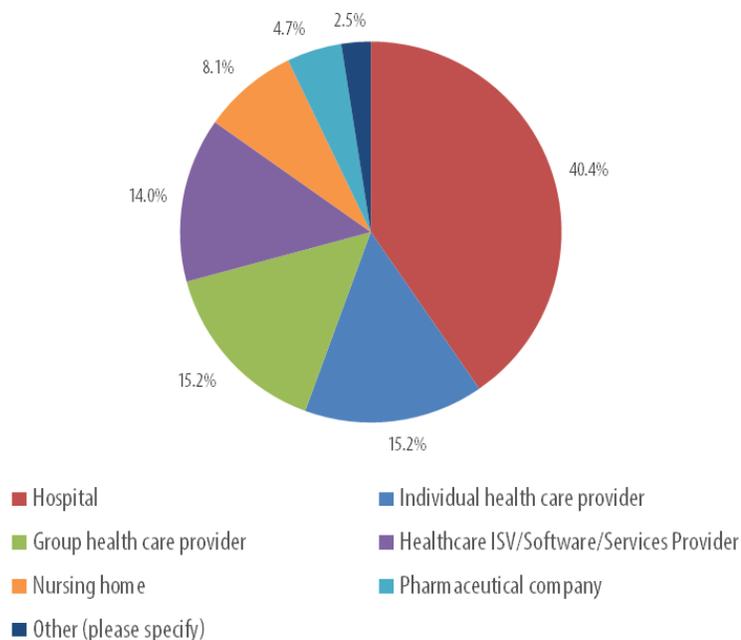
Small	Medium	Large	Total
88	118	116	322

# Respondent Mix

Company Size



Company Type



- Survey respondents came from a variety of different health care organization sizes and types
- Roughly 80% were employees of direct health care organizations, such as hospitals, individual health providers and nursing home
  - Others came from organizations, such as pharmaceutical companies, that are part of the larger health care industry

# Summary and Conclusions

# Health Care IT An Interesting Blend

- The health care industry carries elements of both conservatism and progressiveness when it comes to their approach to IT
- Given the very real privacy concerns and heavy regulation surrounding personal health records, many of their policies regarding devices are, understandably, quite conservative
  - Overall BYOD adoption, for example, is decent, but less than 21% of companies have formal BYOD policies
  - The vast majority of active compute devices in health care are still purchased and managed by the business
- At the same time, nearly 60% of health care organizations are either actively trying or considering leveraging the data from their patient's wearable devices over the next two years

# Security and Privacy are Key

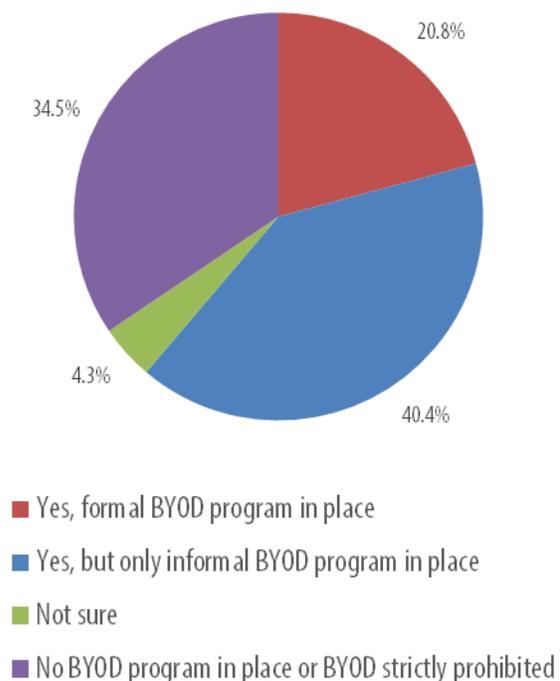
- Many organizations have very tight and restrictive controls over BYOD devices
  - Roughly half reserve the right to pull all data off of personally-purchased PCs or tablets at any time and 43% have a similar policy for BYOD smartphones
  - Just under half have policies that enable them to completely wipe all data (including personal data) off of BYOD PCs and tablets with a 40% response rate for smartphones
    - In fact, slightly more companies have policies to wipe all data than have policies to wipe only corporate data
- Between 85% and 90% of respondents use some type of encryption on the PCs in their organization, with slightly more than half of that group using full-disk encryption versus data-only encryption methods
- 41% of organizations use multi-factor authentication with smart cards and many other organizations are also investigating biometric solutions and other multi-factor solutions
  - Very few seem willing or able to completely rid themselves of passwords, however

# Application Development and Control

- Health Care IT has been relatively slow at building custom mobile applications for smartphones and tablets, with well more than half of all respondents saying they had no plans to do so
  - Companies who are building them are more likely to enable them on company-purchased devices than on BYOD devices
  - The most common type are standalone apps built specifically for native mobile OS's
- Over 50% of respondents have policies that force the installation of certain required applications on BYOD PCs and tablets and 36% require them on smartphones
  - A similar, but smaller number (49% for PC, 40% for tablet and 24% for smartphones) have policies that block certain applications from being installed on BYOD devices

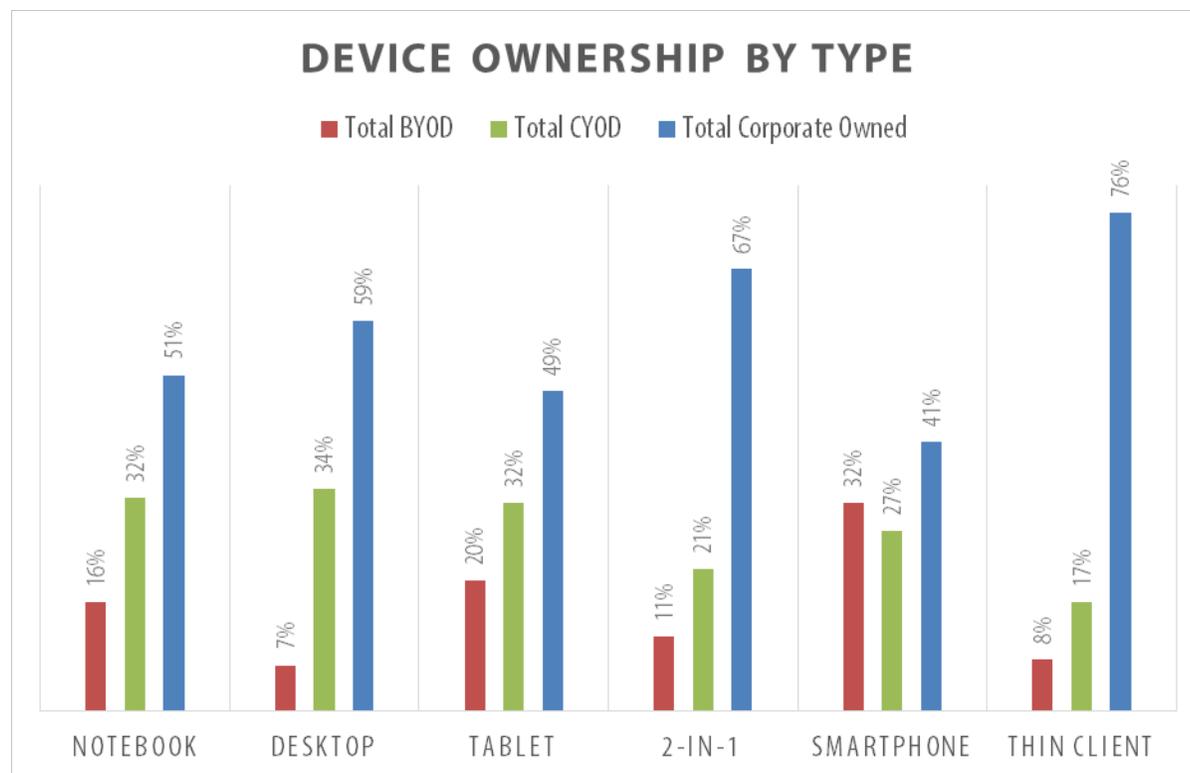
# BYOD Adoption

BYOD Policies



- Just over 60% of total health care IT respondents said they had either a formal or informal BYOD policy in place, but only 1/3 of those had a clearly articulated policy
- Over 1/3 of the total said BYOD is not available or prohibited, reflecting concerns about privacy and security of patient data

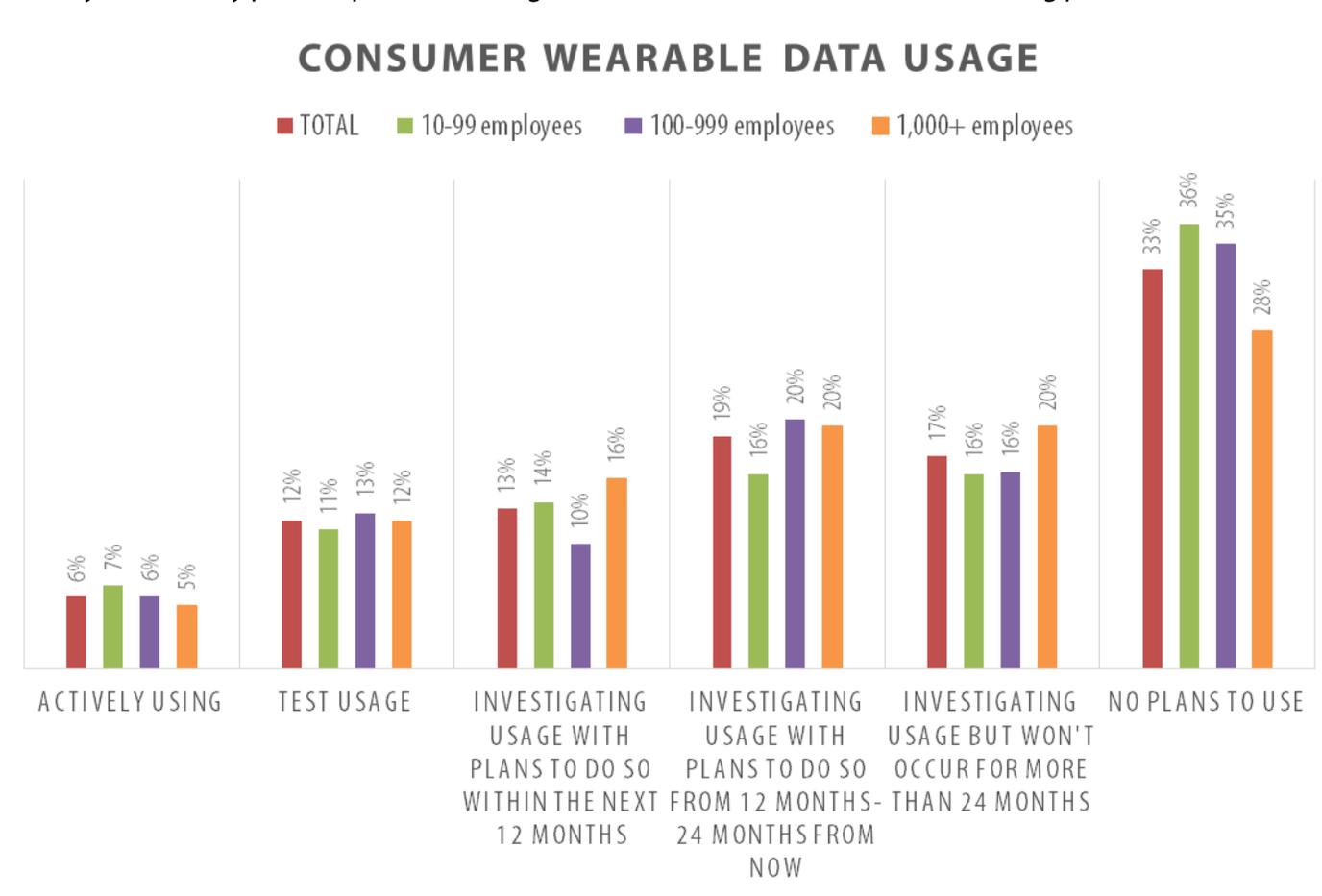
# Device Ownership by Type



- Most devices in active use in health care organizations are purchased and owned by the business
- Not surprisingly, smartphones are the category with the highest BYOD usage
- The most popular categories for CYOD were PCs and tablets, with about 1/3 of total devices fitting into this purchase model

# Leverage Consumer Wearables for Data Collection

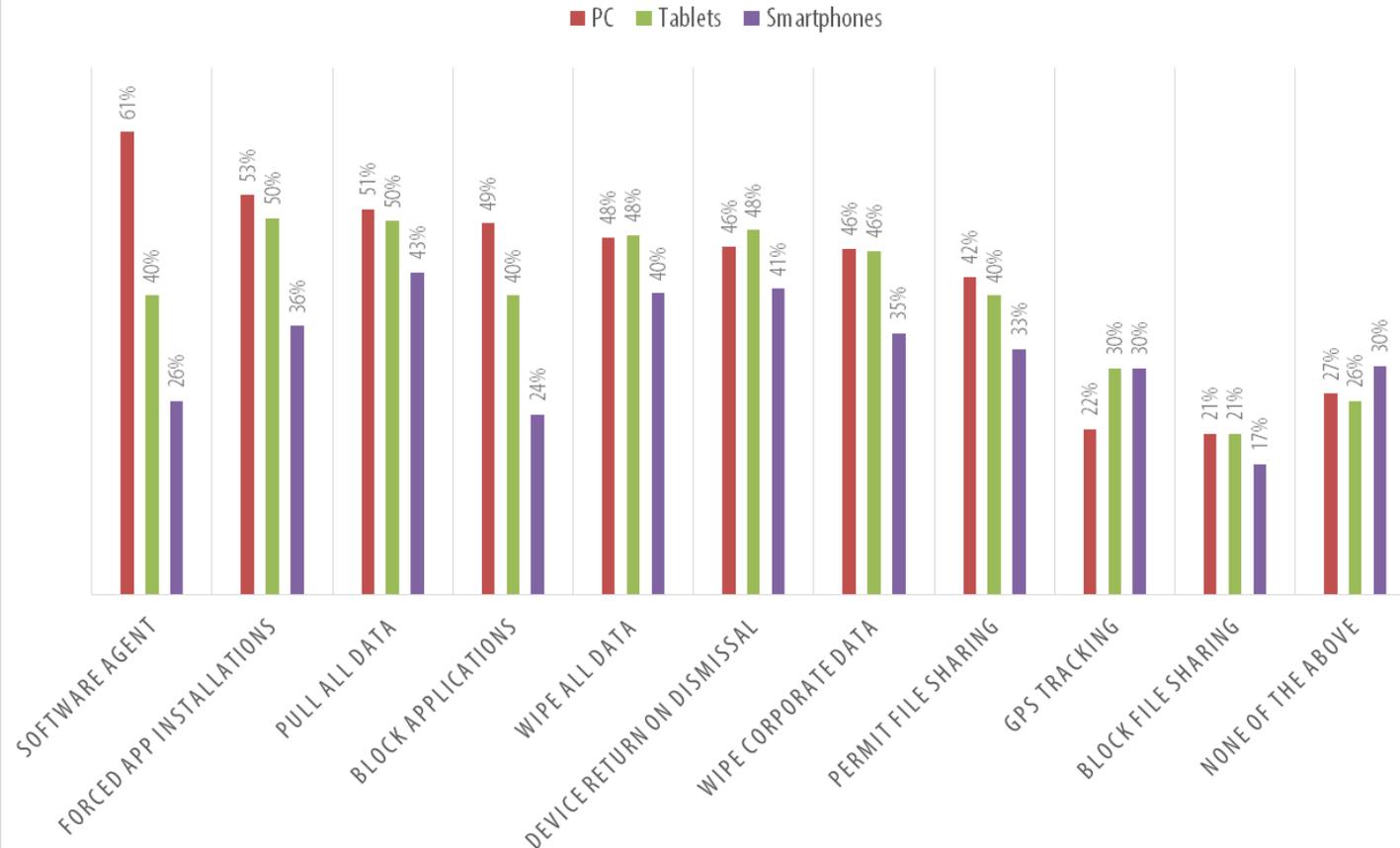
Q. Do you have any plans in place to leverage consumer wearable devices for collecting patient data?



- A mere 6% of respondents said they were actively using patient data from consumer wearables already, but there was clearly strong interesting in pursuing the idea, as a total of 60% of respondents were already testing usage or planning to do so over the next two years
- A third of total respondents said they had no plans to leverage this data, but only 28% of larger businesses said the same, suggesting a strong opportunity for device makers and health care organizations to get together and develop these kinds of links

# BYOD Device Management Policies

MANAGEMENT POLICIES BY DEVICE TYPE



- Management policies for BYOD devices vary widely by device type with software agents being most common on PCs at 61%
- Forced app installations occur in over half the organizations that were surveyed
- Concerns about lost data drive very high usage of remote wipe policies on tablets (48%) and phones (40%)
- Many organizations (over half for PCs and tablets) also reserve the right to pull all data from the device at any time

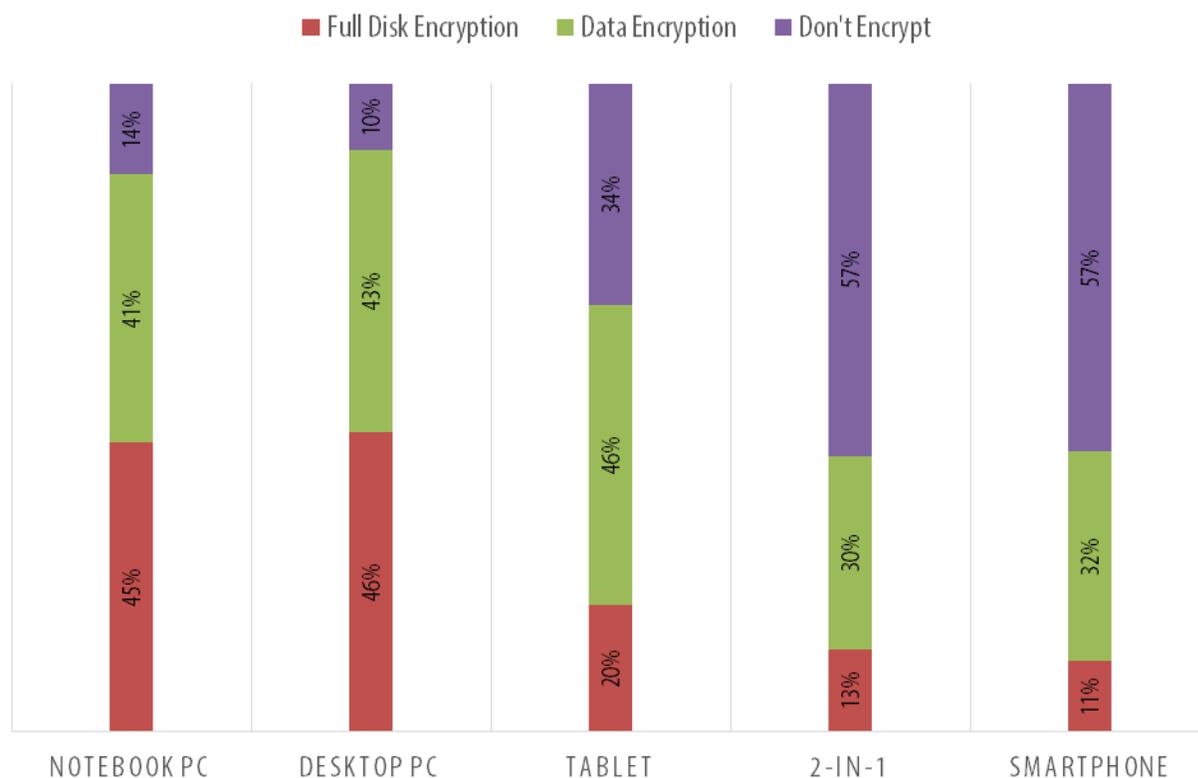
# Security Methods in Use



- While there's great frustration with passwords, they are still the top authentication method by far
- Smart cards were cited by 41% as being in active use
- Biometric usage was lower, but there was greater interest in it for future deployments
- Very few organizations have any plans to get rid of passwords entirely

# Data Encryption Methods

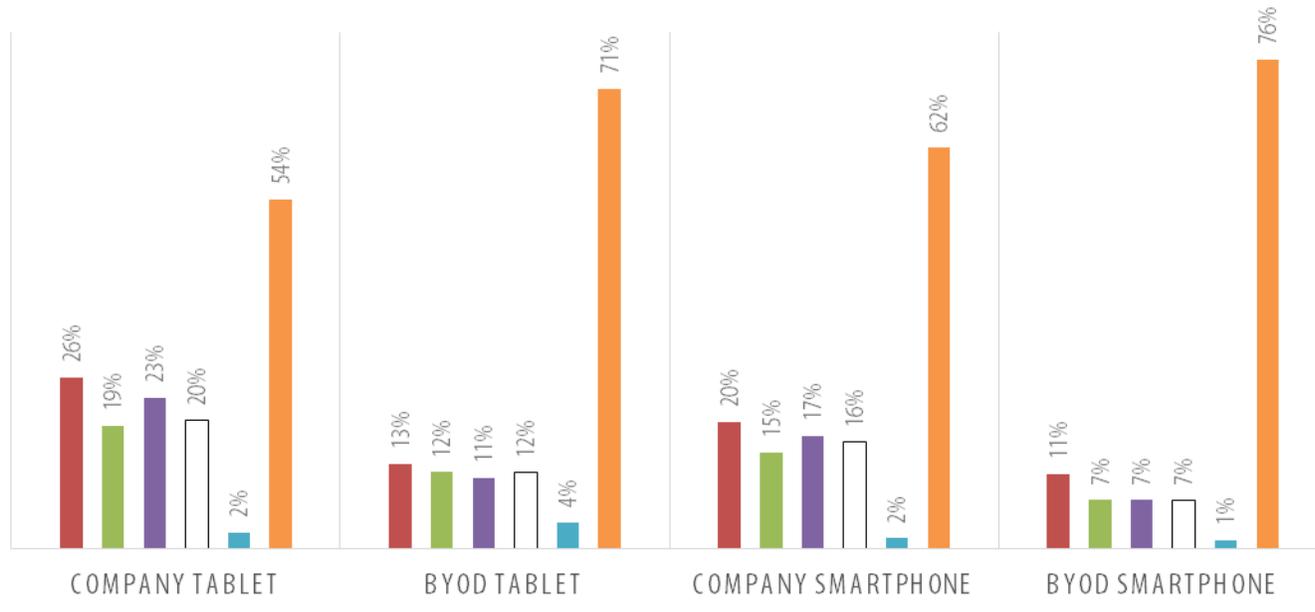
ENCRYPTION METHODS BY DEVICE TYPE



- A very high percentage of PCs (85-90%) and a respectable 66% of tablets are being encrypted, but less than ½ of 2-in-1s and smartphones are
- On PCs, there's still a strong preference for full disk encryption, while on tablets, 2-in-1s and smartphones, there's more usage of data encryption tools

# Custom Mobile Apps

## CUSTOM MOBILE APP PLANS BY DEVICE TYPE



- Most health care organizations are moving slowly to develop custom mobile applications
- For the organizations that are, they're roughly twice as likely to develop them for devices they purchase and own as they are for BYOD devices
- Of the apps that are being built, the most common are those being create as standalone apps to run in native mobile operating systems

# Conclusions

- Health care organizations are being challenged by developments like BYOD
  - While there seems to be some level of interest there, overriding concerns about security and privacy—particularly in light of HIPPA regulations—are forcing them to put in strict policies around these devices
  - Companies that can offer solutions which help mitigate these fears, but enable them to offer the kinds of flexible solutions that many medical professionals want, could clearly benefit
    - Better and more widespread deployment of virtualized “containers,” for example, could help enable health care IT from mandating some of their more draconian management policies
- Mobile devices can clearly be beneficial for medical professionals who are constantly moving around in places like hospitals, yet it’s clear that many IT organizations don’t have the tools they need and/or are used to for mobile devices
  - Overall adoption of critical management and security policies are much lower on smartphones than they are on tablets and those are still lower than PCs
  - This is clearly another important opportunity for vendors to target

“With such a big organization, it is important to keep a handle on all data and devices. It can get overwhelming with BYOD, so it’s important that our IT staff does its due diligence and maintains a strict technology policy.”—Survey respondent

# Conclusions, Part 2

- Despite these concerns, health care organizations are looking to the future and trying to integrate new technologies in innovative ways
  - Many are investigating advanced data center technologies like hyperconverged appliances and cloud-based services
- Though wearables are a brand new category, there's a recognition within Health Care IT that there could be value in being able to leverage their patient's data from these devices.
  - Some organizations are even looking at offering reduced premiums or other benefits to their patients in exchange for this data



“As we migrate more of our infrastructure to Cloud technologies we are facing security challenges that must be overcome to complete the transition. Also on an enterprise level, we are attempting to merge information across multiply platforms. Lots of work ahead.”—Survey respondent

# Contact



Bob O'Donnell  
Founder and Chief Analyst  
TECHanalysis Research, LLC  
1136 Halsey Blvd.  
Foster City, CA 94404

[bob@technalysisresearch.com](mailto:bob@technalysisresearch.com)

(650) 224-2355

[@bobodtech](https://twitter.com/bobodtech)

[www.technalysisresearch.com](http://www.technalysisresearch.com)



**technalysis**  
R E S E A R C H