



WORKSHOP—JUNE 26, 2012

Tweet #NCCoE



# PANEL 3

## Business Community

# NCCoE Proposed Business Model

## Planning Phase

Business  
Engagement &  
Problem  
Statement



Use Case



## Implementation Phase

IT Industry  
Components  
Selection



Implement in  
Operational  
Environment



# Business Community

- User-derived Requirements
- Business Case for Satisfying Requirements
  - Development investment
  - Demand
    - Motivation
    - Potential Market Size
    - Marker Persistence
    - Projected Margin Over Life-cycle
  - Support investment

## Planning Phase

Business Engagement  
& Problem Statement



Use Case



# PLANNING PHASE

- Step 1: *The Business Community proposes the business problem to the NCCoE.*
- Step 2: *The Business Community and Cybersecurity Technologists propose one or more use cases to NCCoE. [Capability that addresses problem]*
- Step 3: *Consumer and NCCoE collaborate to flesh out the use case.*
- Step 4: *NCCoE solicits public feedback on the use case.*
- Step 5: *NCCoE refines the use case based on public feedback and NCCoE knowledge of existing standards and guidelines.*



## PROBLEM STATEMENT

Step 1: *The Business Community proposes the business problem to the NCCoE or the Advisory Board shares with NCCoE a known, current threat within an operational environment.* After identification the NCCoE reviews proposed business problems in an open, transparent manner and selects one or more to be addressed (through use cases) using:

- Known operational business environment
- Current threat environment
- Existing IT component and technologies currently available
- Community's level of interest in the business problem
- The feasibility of use cases that can be developed for the business problem
- Feedback from core organizations in the NCCoE customer's sector
- Feedback from the NCCoE Advisory Board



**Himss**

[www.himss.org](http://www.himss.org)

# Healthcare Privacy and Security Challenge: Mobile Computing at the End Points

**NCCoE Workshop**  
**June 26, 2012**

transforming healthcare through IT™



# Speaker

Lisa A. Gallagher, BSEE, CISM, CPHIMS  
Senior Director, Privacy and Security  
HIMSS

[lgallagher@himss.org](mailto:lgallagher@himss.org)





# Agenda

- Current HHS Breach Data
- Mobile computing landscape in healthcare
- Privacy and security challenges
- Review Mobile Use Survey *m***HIMSS**®
- Review available mobile security resources





# HHS Breach Reporting Data

- As of March 31, 2012 –
  - 409 breaches were reported to HHS where each breach affected 500 or more patients
  - Total number of patients affected by these large breaches: 19,159,770
- Reasons given for the breaches
  - Theft – 54%
  - Loss – 13%
  - Unauthorized Access – 20%
  - Improper Disposal – 5%
  - Hacking – 6%



***Business Associates were responsible for 21% of all reported breaches***



# By the numbers...

Device Type	Number of Incidents	% of Total Incidents	Number of Patients	% of Patients
Laptop	97	24%	1,817,020	9%
Portable Devices	61	15%	1,496,273	8%
Hard Drives	1	0.2%	1,023,209	5%
Desktop Computer	2	13%	2,244,379	12%
Paper Records	105	25%	628,188	3%
Network Servers	48	12%	1,613,024	8%
Backup Tapes	6	1%	5,976,655	31%
E-mail*	8	2%	12,547	0.06%

***In most healthcare organizations today –  
Smart phones are personally-owned***

Data was obtained on March 31, 2012 through the Department of Health and Human Services' website for healthcare organizations reporting breaches which affected more than 500 individuals.



## US Mobile Health Market

- Wireless health market will rise from
- \$2.7M in 2007 to \$9.6B in 2012
- 80%+ physicians in U.S. have smartphone
  - Two-thirds use online content for professional needs
- 95% physicians using handheld devices/smartphones download apps for medical info
- Mobile apps being developed by traditional health care providers , device manufacturers, pharmaceutical manufacturers and researchers around the world.





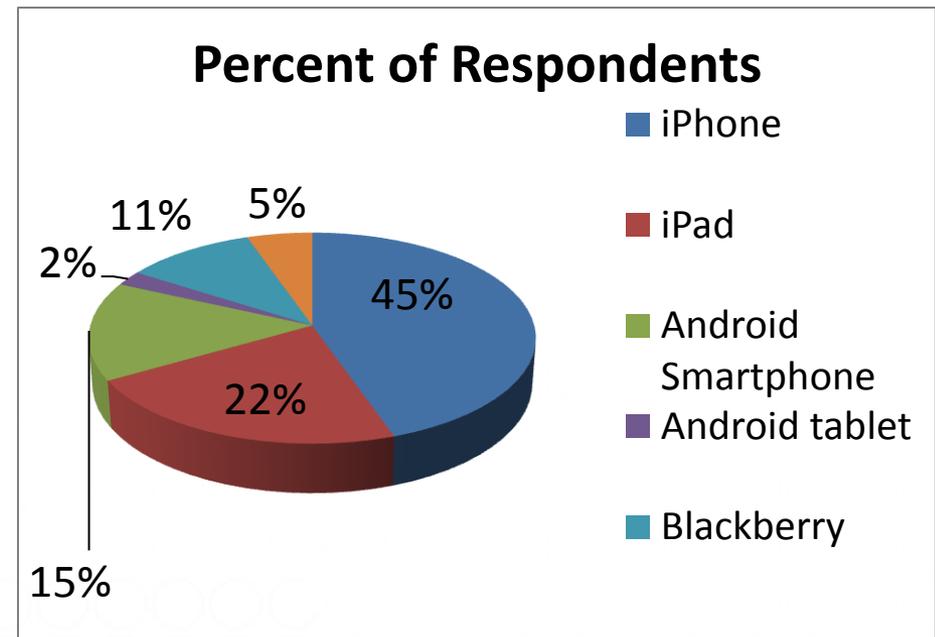
# Number of Health Apps on the Rise

Application	Number of health applications available for download	Intended for consumer/patient	Intended for healthcare professional	Number of downloads
iPhone	~6000	73%	30%	Unknown
Android	~600	81%	20%	3.5 million +
Blackberry	~200	70%	30%	Unknown



# Surprising Find in Study on Physician Smartphone Users

- More than 80% physicians own a mobile device, compared with only 50% of the general U.S. population
- 44% that do not own a mobile device intend to purchase one in 2011
- 25% physicians are using smartphones and tablets in their practices
- Physicians with 20-plus years experience most frequent users of tablets





## And, Use of Mobile Technology is Highly Complex...

- Data exchange requirements
  - Proper, accurate, and confidential collection and protection of a broad range of data
  - These exchanges are not yet tailored to healthcare
- Workflow challenges
  - Smartphones and tablet computing fit with lifestyle, personal, and professional needs of clinicians
  - CIOs facing an onslaught of user demand
  - Tremendous challenges and opportunities to connect with patients and consumers
- **Privacy/Security** continues to be a concern



# Key Mobile Issues

- **Privacy & Security**
- Infrastructure
- Finance & Reimbursement
- Policy & Regulation
- Standards & Interoperability
- Usability & Accessibility
- Infection Control
- Research
- Quality Care & Patient Safety
- Efficiency & Workflow
- Patents, IP, Commerce & Innovation
- Access to Information & Technology



# HIMSS Mobile Survey

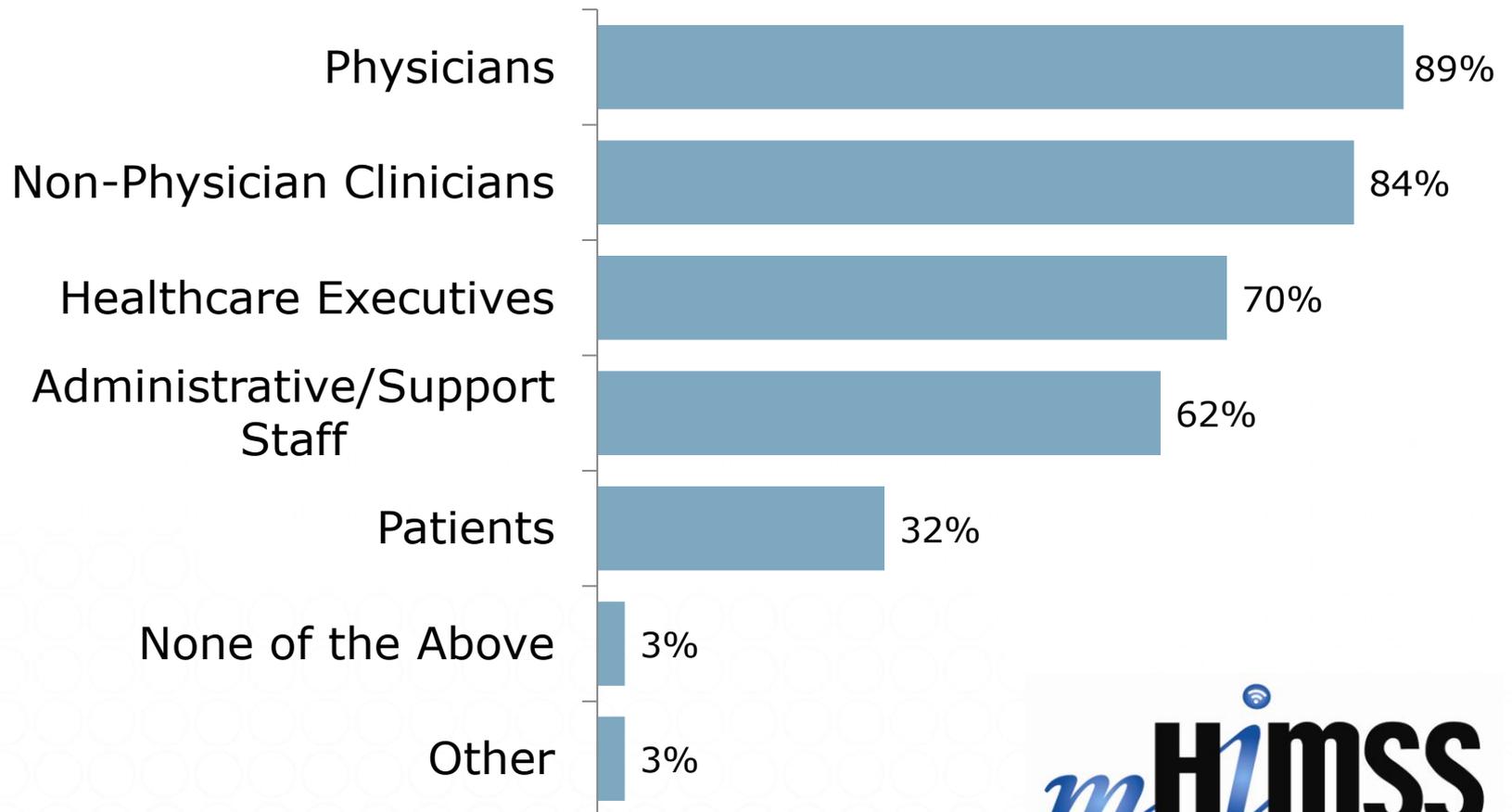
*December 2011*

*Hospital / Health Systems N=164*

- Mobile & wireless technology has advanced quicker and are being adopted faster than hospital policies
- Many hospitals are allowing the use of private mobile & wireless devices without policies & procedures in place
- P&S concerns remain a barrier to adoption & use
- 41 % are allowing use of device owned by the end user
- 28% of devices are retaining PHI
- 77% are accessing data on public networks

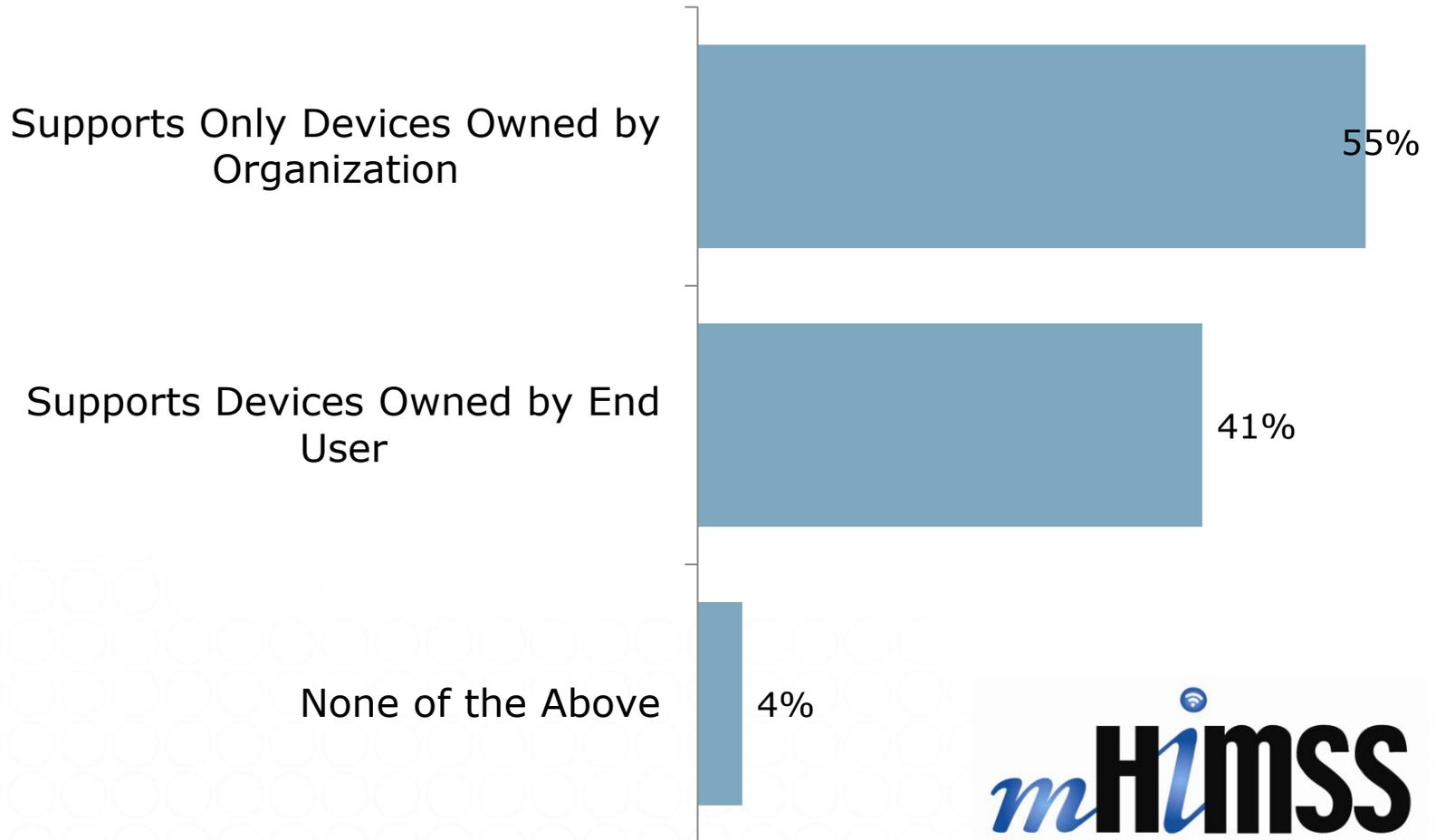


# Professional Groups Using Mobile Devices



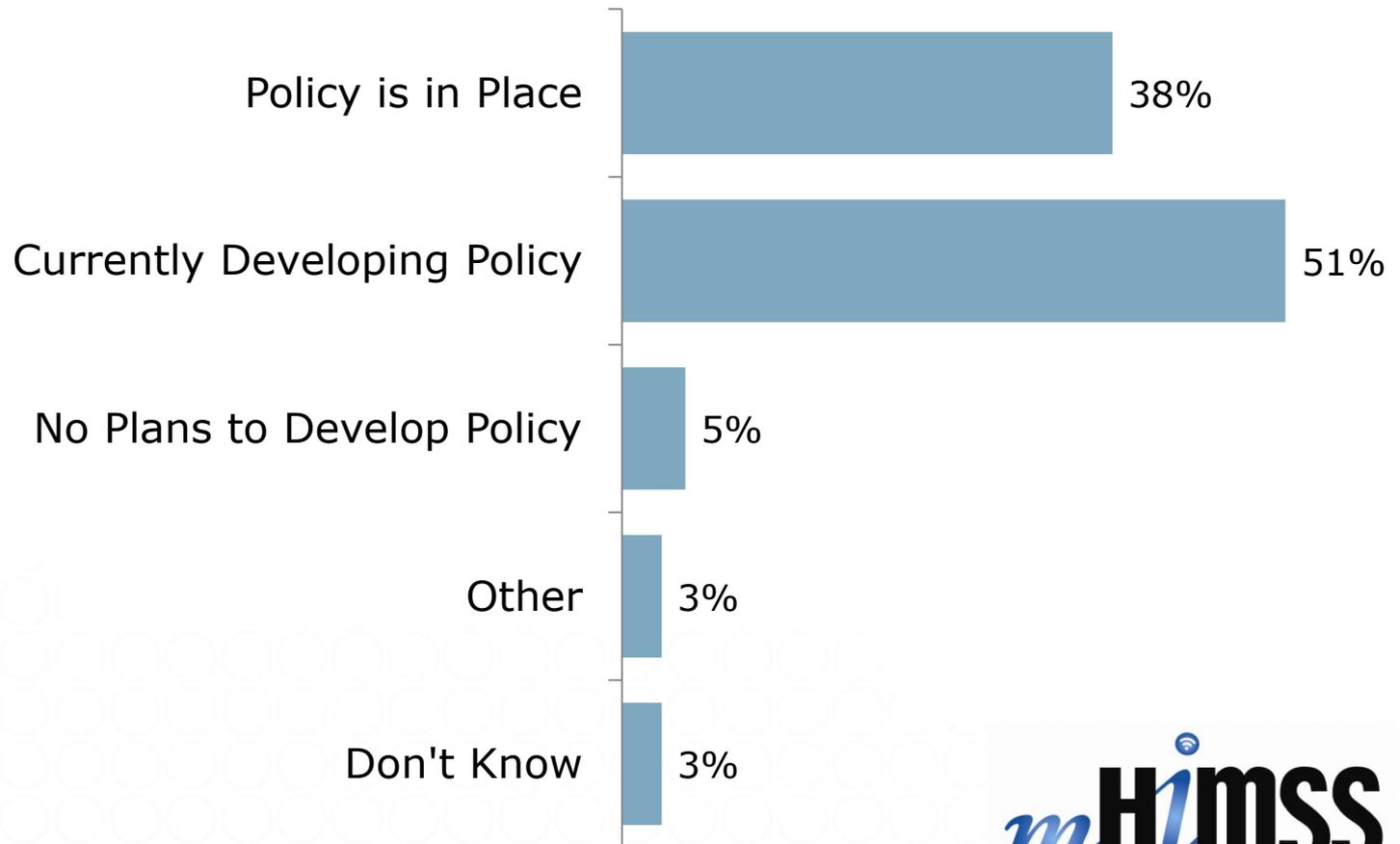


# Organizational Support of Mobile Devices



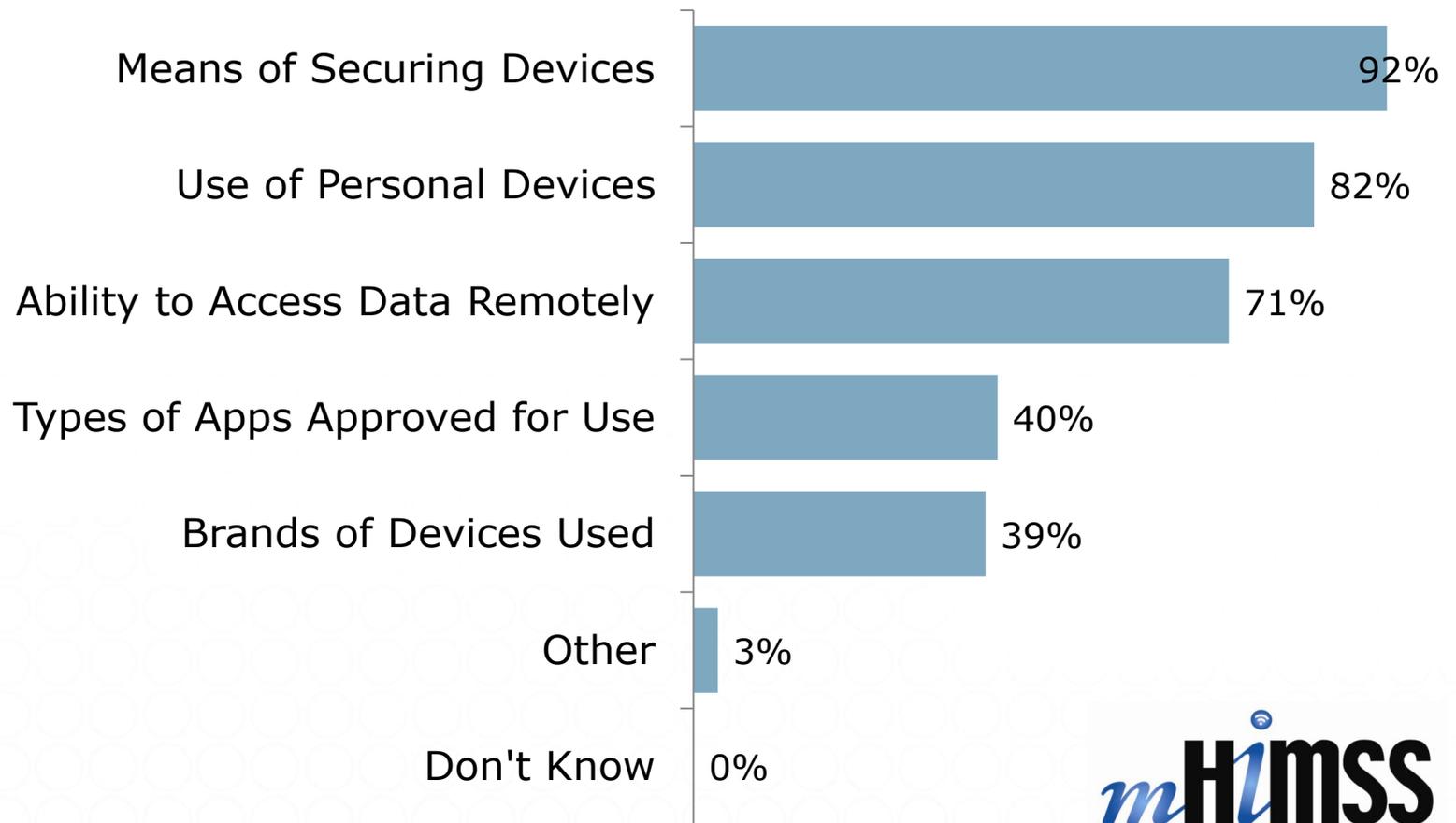


# Mobile Technology Policy



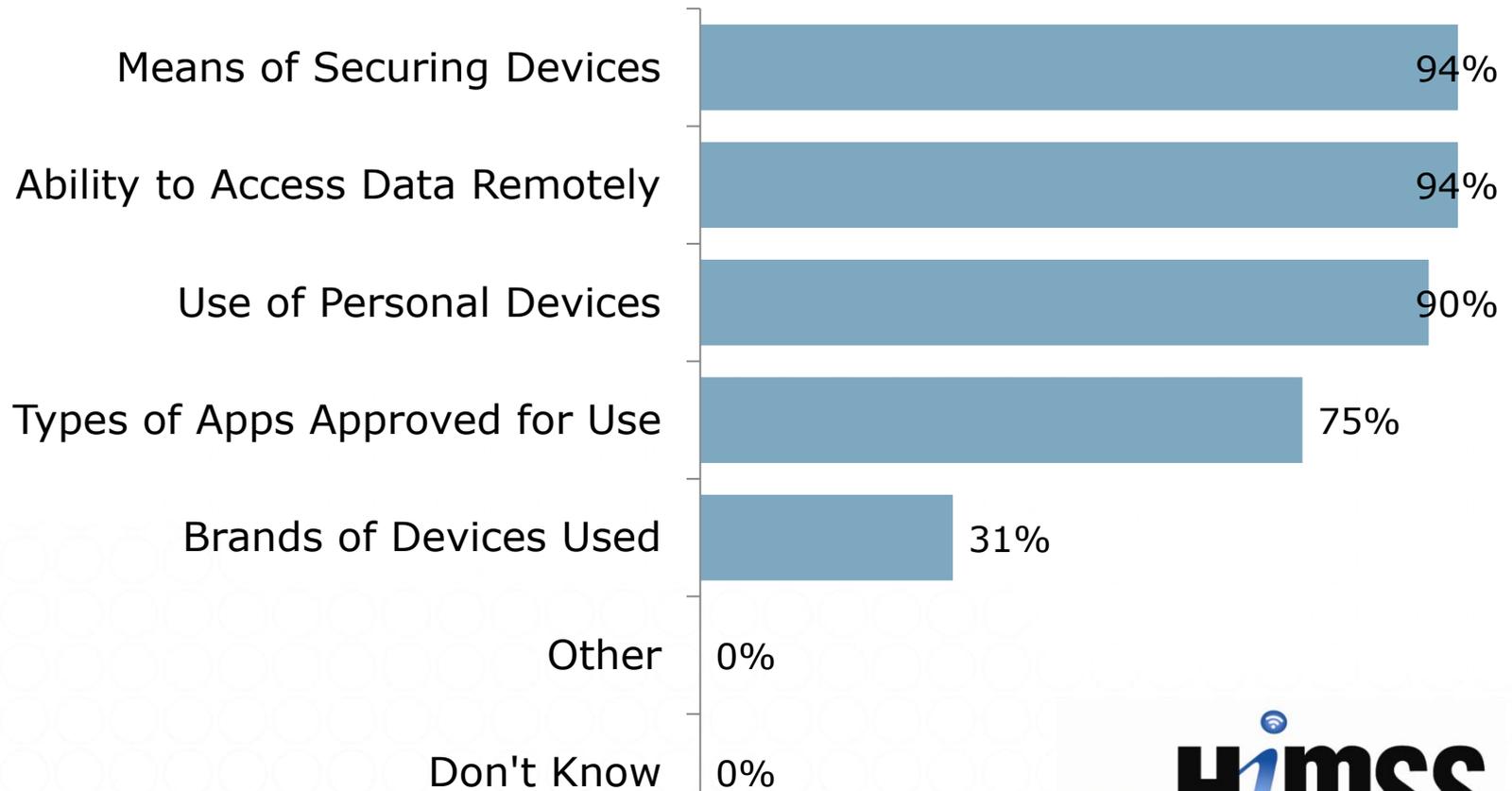


## Areas Addressed by Mobile Technology Policy



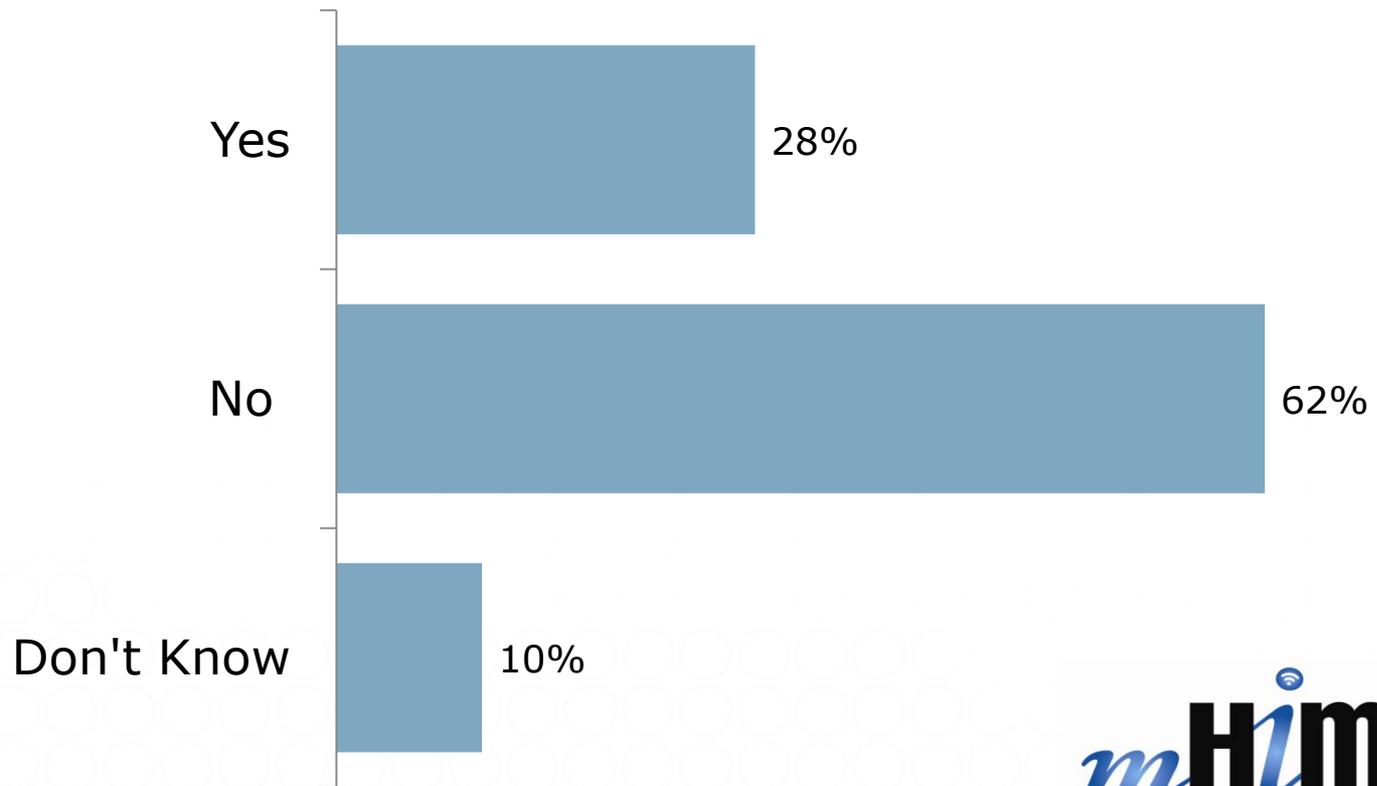


# Areas Addressed by Mobile Technology in Proposed Policy



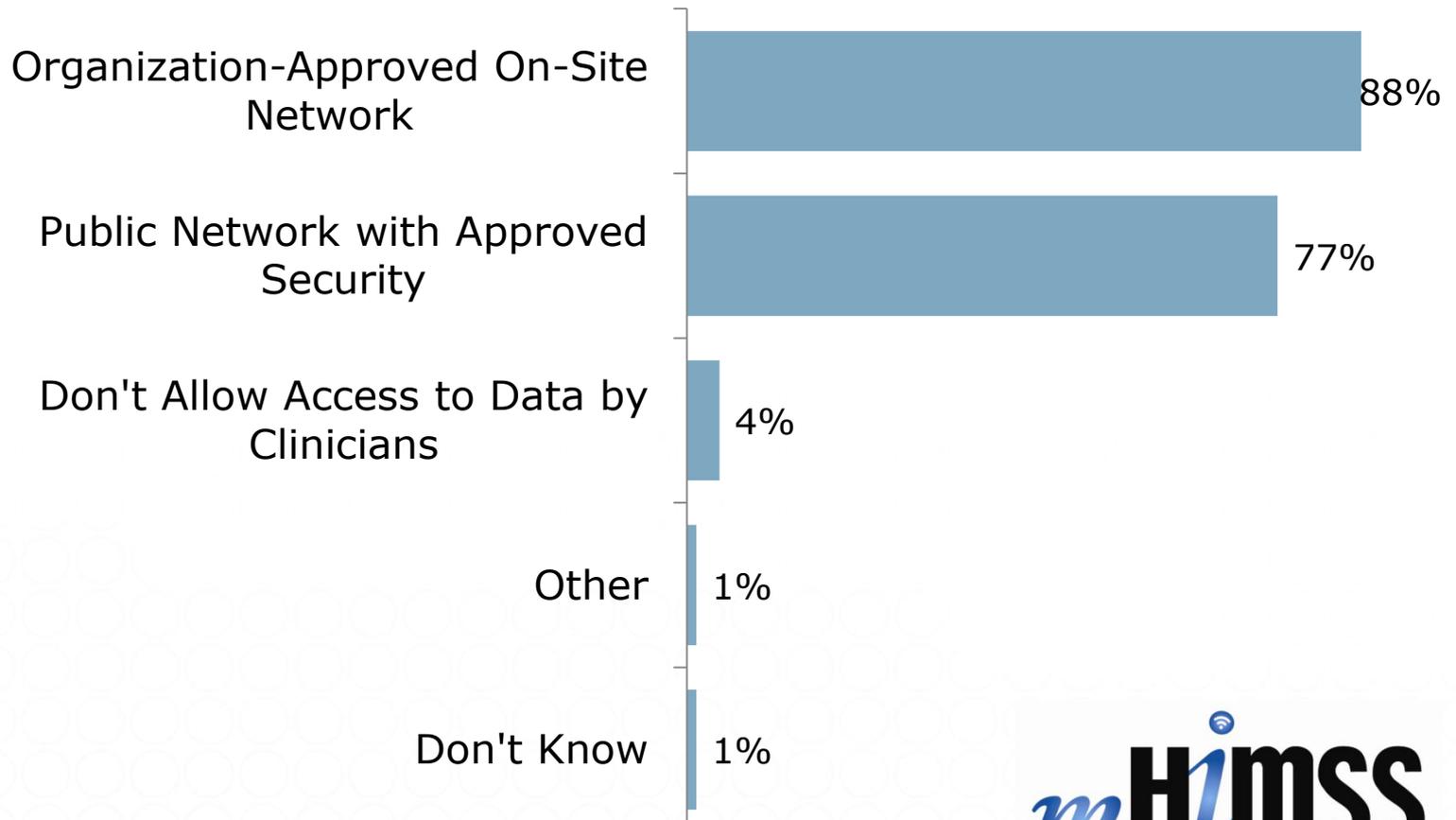


## Mobile Devices Retain PHI



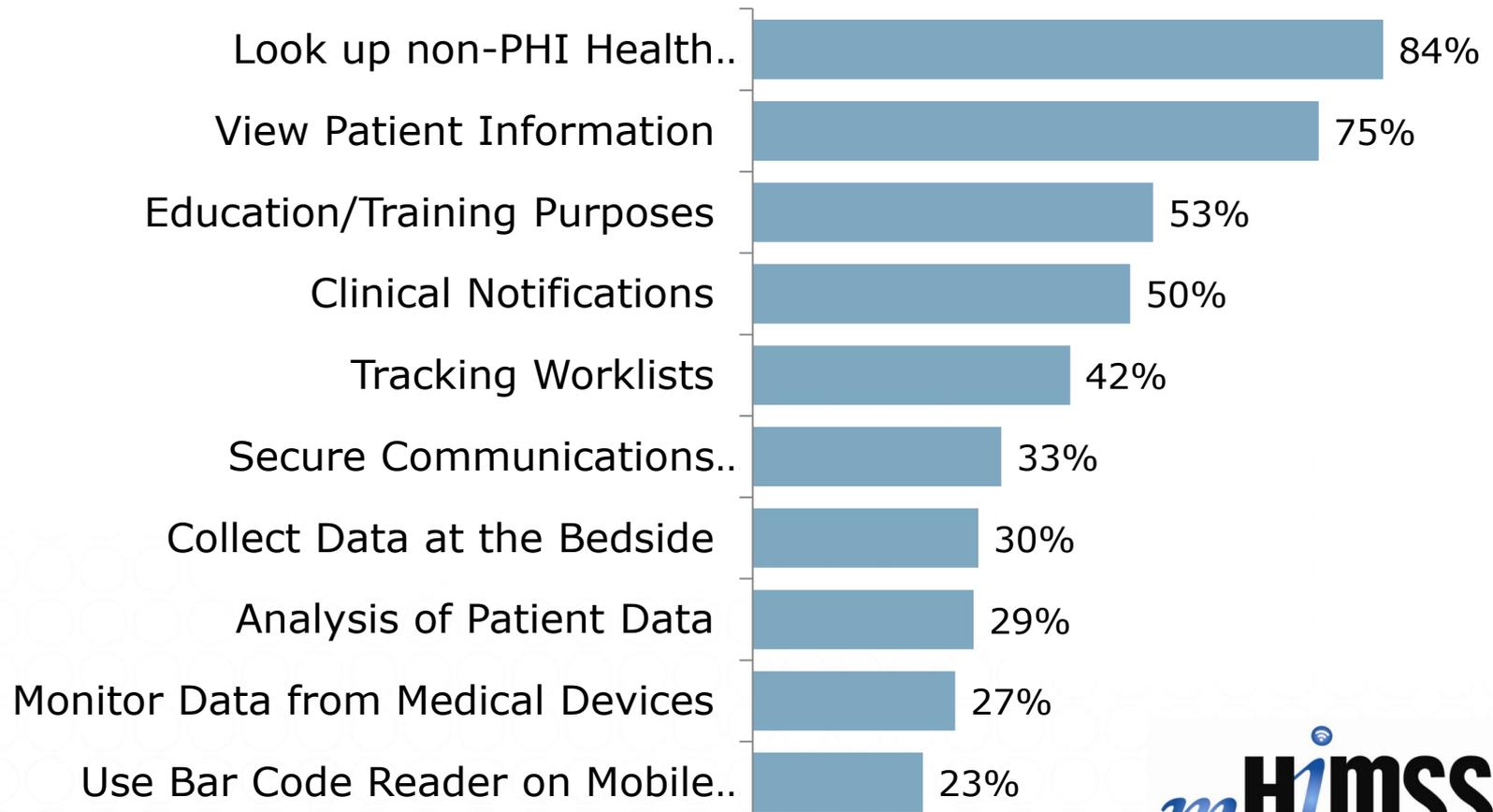


# Locations From Which Clinicians Can Access Data Using Mobile Devices



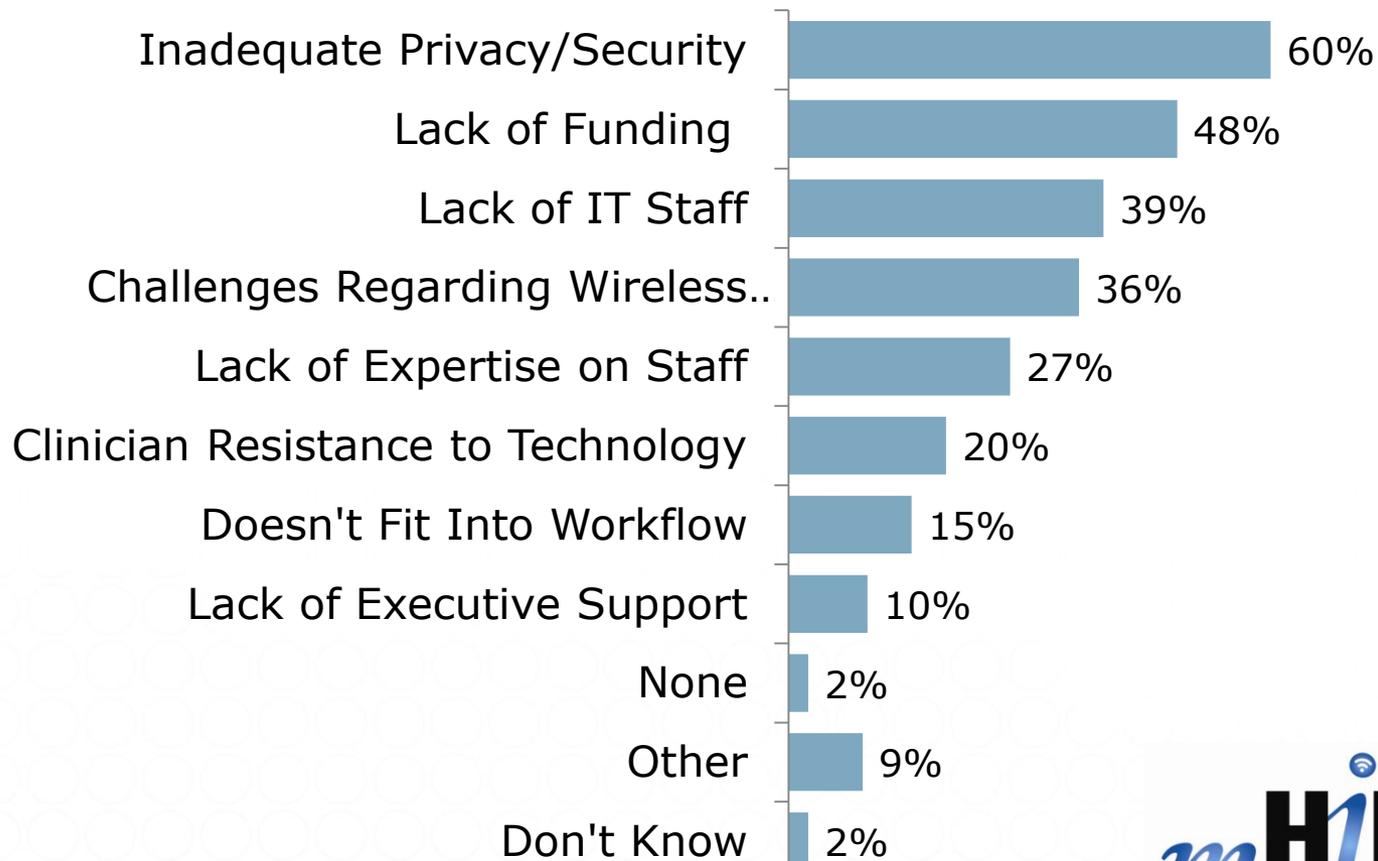


# Clinician Use of Apps Top 10 Responses



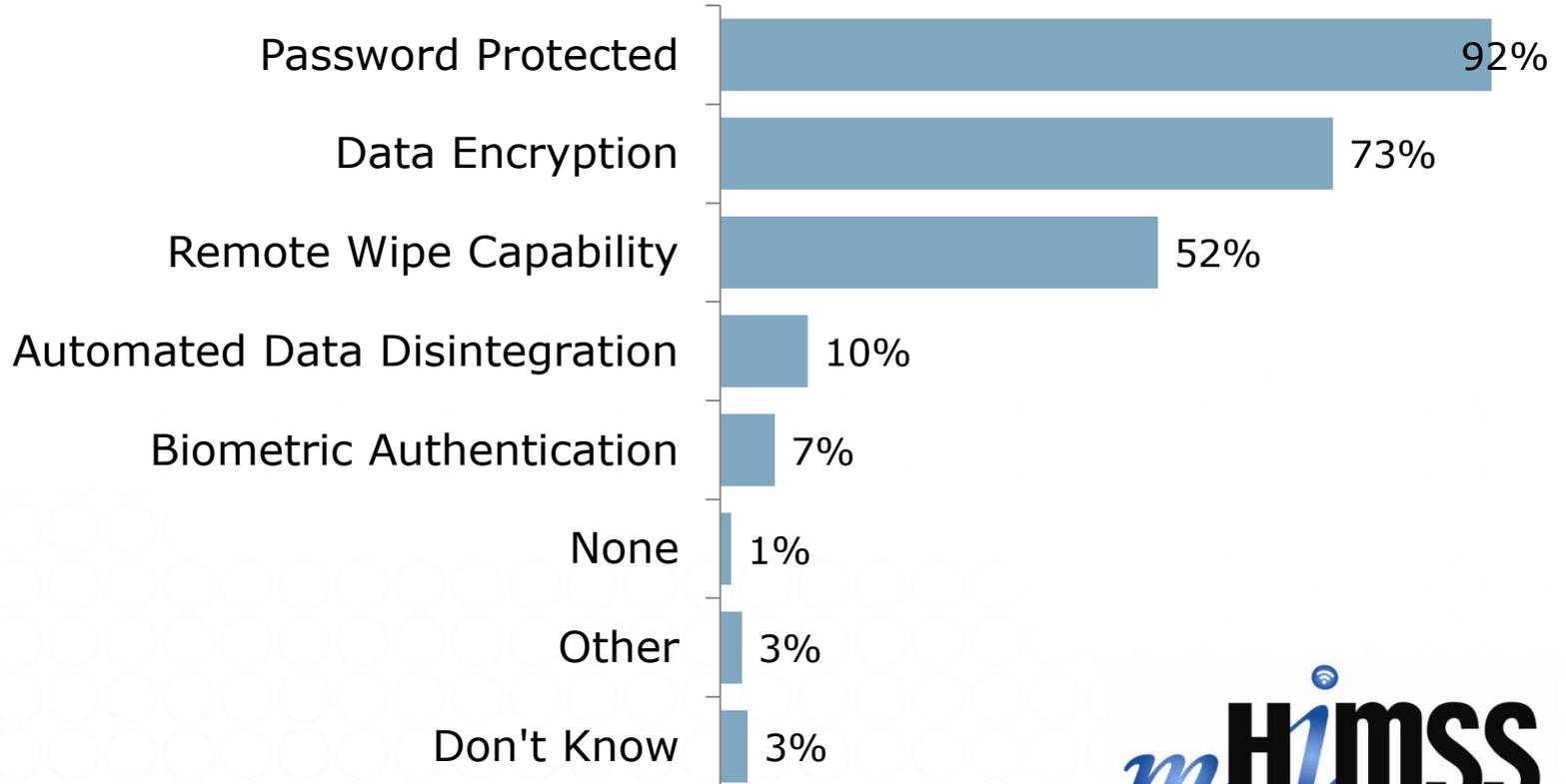


# Barriers to Use of Mobile Technology





# Mechanisms in Place to Secure Data on Mobile Devices





Topics & Tools

Privacy and Security

Overview

HIMSS Annual Security Survey Results

Legal and Regulatory

Information Systems Security

Medical Identity Theft

Privacy Impact Assessment

Privacy & Security for RHIOs/HIEs

Privacy and Security for Personal Health Records

Privacy & Security Committee, Task Forces and Work Groups

Resources from our Corporate Members

Medical Device Security

Privacy & Security Toolkits

News

## Privacy & Security Toolkits

Be prepared for healthcare IT challenges with HIMSS Privacy and Security Toolkits. Each Toolkit contains resources, best practices and case studies on a variety of important privacy and security topics. Begin exploring today!

**Privacy & Security Toolkit**  
Outlines general principles and examples of how healthcare entities can manage the privacy and security of their electronic information to meet compliance requirements.

**Privacy & Security Toolkit for Small Provider Organizations**  
Smaller organizations will find guidance in this toolkit for implementing an appropriate set of policies and procedures for their organization.

**Patient Identity Integrity Toolkit**  
Learn about patient identity integrity and the many issues involved in reliably and safely matching patient identity across systems.

**Risk Assessment Toolkit**  
Learn how to conduct security risk assessments and implement a risk management process in your healthcare organization.

**Mobile Security Toolkit**  
Manage the security of mobile technologies in your healthcare IT environment based on industry best practices.

**Cloud Security Toolkit**  
Understand cloud computing and its associated security challenges to make informed

Share | Facebook | Twitter | LinkedIn | Email

@HIMSS  
Sign up to learn more about HIMSS. Enter your email address below.

submit

ADVERTISEMENT

MASTER of SCIENCE IN  
HEALTH INFORMATICS &  
MANAGEMENT SYSTEMS

FIU | Business  
FLORIDA INTERNATIONAL UNIVERSITY

SMARTER HEALTHCARE.  
STARTING FALL 2012.

Reboot.

BE A PIONEER.  
Lead the change in



Windows Internet Explorer browser window showing the HIMSS website. The address bar contains [http://www.himss.org/ASP/topics\\_PStoolkit\\_MobileSecurity.asp](http://www.himss.org/ASP/topics_PStoolkit_MobileSecurity.asp). The page title is "HIMSS | Mobile Health Security Toolkit | mHealth | mHIMSS".

The website header includes the HIMSS logo and navigation links: Home | About HIMSS | Contact Us | Member Login. A search bar is also present.

The main navigation menu includes: News & Research, Topics & Tools, Professional Development, Conference & Events, About Membership, and HIMSS Store.

The "Topics & Tools" section is active, displaying the "Mobile Security Toolkit" with a wrench icon. The content area includes:

- Introduction & Industry Overview**: The HIMSS Mobile Security Toolkit assists healthcare organizations and security practitioners in managing the security of their mobile computing devices.
- Guidance & Implementation**: As the healthcare community becomes more sophisticated in its adoption and use of information technology systems, organizations are increasingly making use of mobile technologies to meet the demands of their employees and increase workflow efficiencies.
- Bring Your Own Device & Consumerization**: This Toolkit will help you understand the security risks and issues associated with incorporating mobile devices into your organization, and how to develop mobile security policy implementations for corporate and personally-owned devices. It contains resources with tips on securing your wireless network, smartphones and other mobile devices.
- Wireless, Smartphones & Applications**: [Get Started - Introduction to Mobile Security](#)
- Regulatory & Legal Information**: [More Toolkits - Privacy & Security Toolkits Directory](#)
- mHIMSS**: [Got feedback? Send comments & submit ideas for new content!](#)
- More Privacy & Security Toolkits**
- Back to Privacy & Security Home**

At the bottom of the content area, there is a **mHIMSS** logo and text: "For more information on mobile in healthcare visit [mHIMSS](#) - an initiative entirely focused on transforming healthcare through mobile technologies." and "Join the mHIMSS mobile community today - Free to current HIMSS individual members!"

On the right side of the page, there is a social media share section with icons for Facebook, Twitter, and LinkedIn, and an email sign-up form with the text "@HIMSS Sign up to learn more about HIMSS. Enter your email address below." and a "submit" button. Below the form is the text "ADVERTISEMENT".



HIMSS - Bring Your Own Device & Consumerization - Windows Internet Explorer

http://www.himss.org/ASP/topics\_FocusDynamic.asp?faid=652

File Edit View Favorites Tools Help

Favorites FoxNews.com - Breaking Ne... Web Slice Gallery Customize Links Free Hotmail Windows Windows Marketplace Windows Media

HIMSS - Bring Your Own Device & Consumerization

Visit these other HIMSS sites: select one

Member Center | Advocacy & Public Policy | Vendor Center | Press Room | HIMSS Blog

search

Home | About HIMSS | Contact Us | Member Login

News & Research | Topics & Tools | Professional Development | Conference & Events | About Membership | HIMSS Store

Topics & Tools

Mobile Security Toolkit

Introduction & Industry Overview

Guidance & Implementation

Bring Your Own Device & Consumerization

Wireless, Smartphones & Applications

Regulatory & Legal Information

mHIMSS

More Privacy & Security Toolkits

Back to Privacy & Security Home

## Bring Your Own Device & Consumerization

This section provides background information, benefits, concerns and guidance needed for healthcare organizations to make informed decisions on how to appropriately address the use of consumer-owned mobile devices in the workplace.

[Considerations for Employee-Owned Mobile Devices](#)

[Sample Mobile Device User Agreement](#)

[Mobile: How to Say 'Yes' Securely](#)

[Security Challenges BYOD Presents](#)

[BYOD: Get Ahead of the Risk](#)

Share | Facebook | Twitter | LinkedIn | Email

@HIMSS

Sign up to learn more about HIMSS. Enter your email address below.

submit

ADVERTISEMENT



## Mobile Resources

- **mHIMSS**® [www.mHIMSS.org](http://www.mHIMSS.org)
- **mHIMSS**® mHIMSS Mobile Survey  
[http://www.himss.org/content/files/2010\\_HIMSS\\_SecuritySurvey.pdf](http://www.himss.org/content/files/2010_HIMSS_SecuritySurvey.pdf)
- **mHIMSS**® The Future of Mobile Technologies and mHealth: Staying Securely Connected: A HIMSS Virtual Forum  
[http://www.himssvirtual.org/20120426\\_VF\\_PrivacySecurity/index.asp](http://www.himssvirtual.org/20120426_VF_PrivacySecurity/index.asp)
- **mHIMSS**® 2012 mHealth Summit  
<http://www.mhealthsummit.org/index.php>
- HIMSS Mobile Security Toolkit  
[http://www.himss.org/ASP/topics\\_PStoolkit\\_MobileSecurity.asp](http://www.himss.org/ASP/topics_PStoolkit_MobileSecurity.asp)



# Business Community Insights

Ilene Yarnoff – Booz Allen Hamilton

Lisa Gallagher – Healthcare Information  
and Management  
Systems Society