Mobile Device Management… Not Simply a “Nice to Have”

R. Greg Manson, CISA

NCHICA Security Workshop
16-Sep-15

Carolinas IT
Experience
Peace of Mind

Session Objectives:

- ePHI Threat Environment
- Mobile Device Usage
- Mobile Device Management (MDM)
- Choosing a MDM Solution

ePHI is the target!

- **Criminal attacks were the root cause in 45% of ePHI data breach incidents**

- **Criminal attacks on covered entities and BAs has increased 125% since 2011**

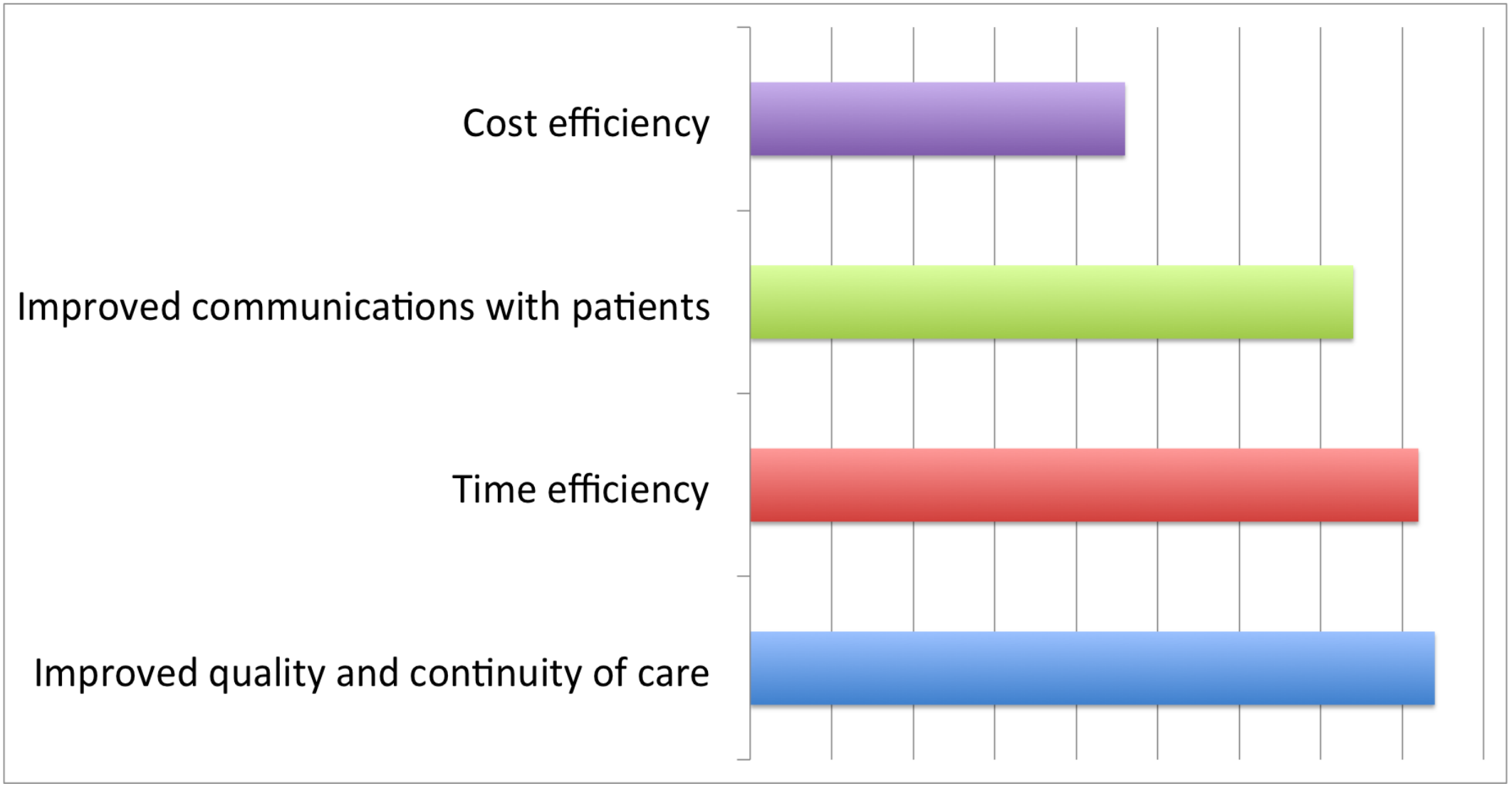
Ponemon Institute 2015 Privacy and Security Report

HIPAA Security by the Numbers

- Black-Market Value: $50/medical record – FBI
- 17,000 Patient Records Breached Per Day – HHS.gov
- Cost per Breached Record: $188 - Ponemon
- HIPAA Penalties for a Lost Unencrypted Laptop: $1.5M – OCR
- Loss of Patient Trust: 56% - Ponemon

90% **of healthcare providers maintained mobile devices to engage with patients** – 2015 HIMSS Mobile Technology Survey

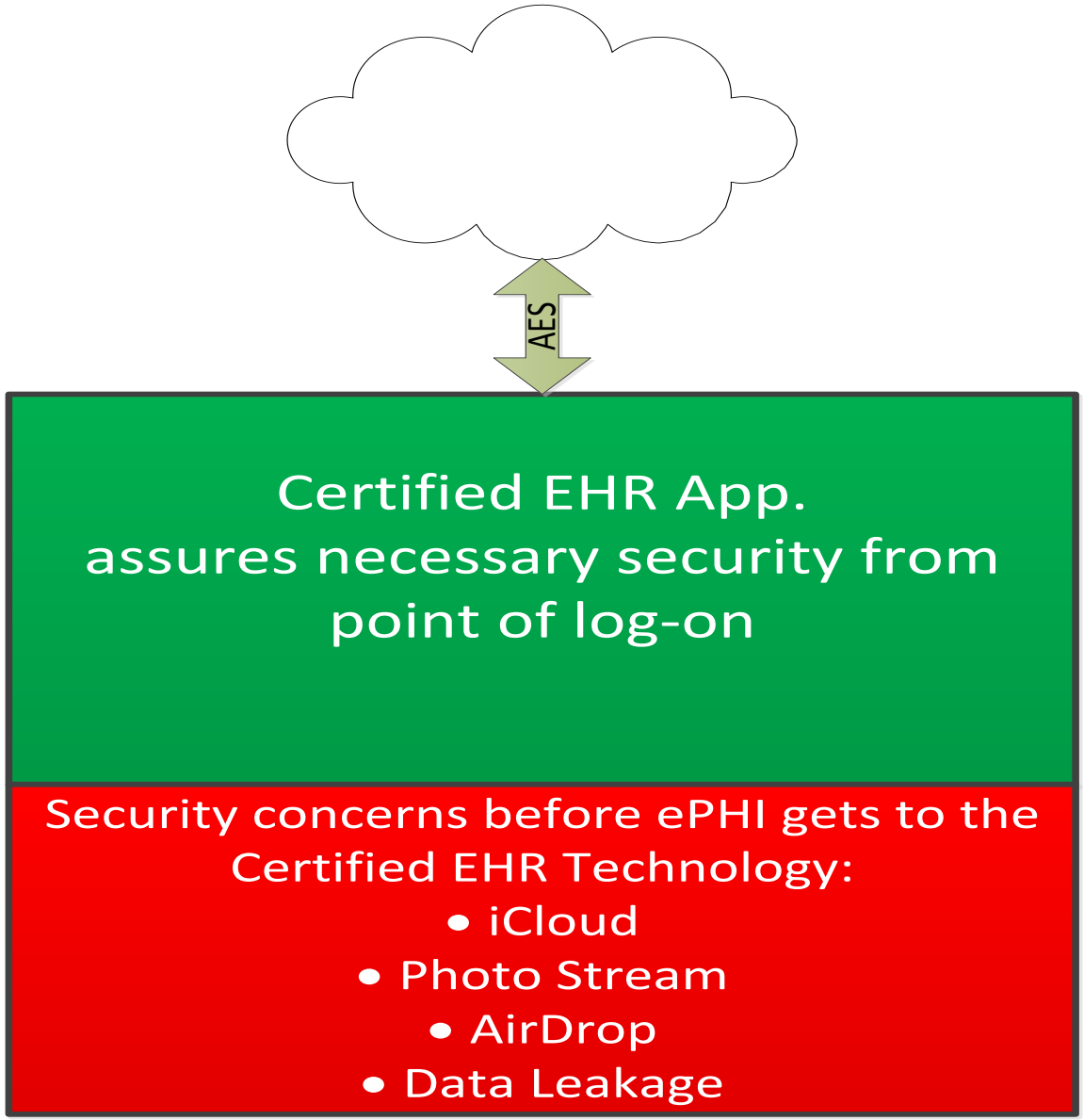
Why?



- MedData Group

Think You Are Safe?

Security Concerns with a Certified EHR App



Gaining Control with MDM

- Enabled Restrictions on Native Functionality
- Enrollment and Inventory
- Restricting app downloads to trusted sources (App Store, Google Play, Private Secured Store)
- Quarantine “jail broken” devices
- Locate and Wipe
- Push Apps and OS Updates

The Best MDM Solution

- Policy requiring Enrollment
- Multiple Profiles (Org-Owned, BYOD, etc.)
- Cloud-Based Dashboard (business continuity)
- App and OS Test Sandbox
- If + Then Quarantine (failed login, geo-fencing)
- Logging


KEEP
CALM
AND USE
MOBILE
DEVICE
MANAGEMENT

Thank You!

R. Greg Manson
Greg.Manson@CarolinasIT.com
919-573-4084

1600 Hillsborough Street
Raleigh, NC 27605
www.CarolinasIT.com

Carolinas IT
Experience
Peace of Mind