Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

# HIPAA Requirements and Mobile Apps

OCR/NIST 2013 Annual Conference

Adam H. Greene, JD, MPH
*Partner*, Washington, DC

# Use of Smartphones and Tablets Is Growing

INSERT BORING STATISTICS HERE.

# How Info Sec Sees Smartphones

Easily Lost, Stolen, or Discarded with PHI on It

Camera for Improperly Recording PHI

No Physical Keyboard for complex passwords

Easy Access to Facebook for Improperly Posting PHI

# How Info Sec First Responds

1. Thou Shall Disable Thy Smartphone Camera
2. Thou Shall Not Text
3. Thou Shall Not Place PHI on Thy Smartphone or Tablet

# How Clinicians and Other Staff Respond

# Design an Effective Mobile App Strategy

1. Identify mobile app needs
2. Integrate into risk analysis
3. Design risk management strategy
4. Obtain business associate agreement if necessary and perform due diligence
5. Document Security Rule compliance
6. For patient/enrollee-facing apps, comply with Privacy Rule

# Identify Mobile App Needs

1. Thou Shall Disable Thy Smartphone Camera

- Is there appropriate use of smartphone cameras for certain procedures?
- Is their an appropriate way to securely share pictures and add them to the record?

# Identify Mobile App Needs

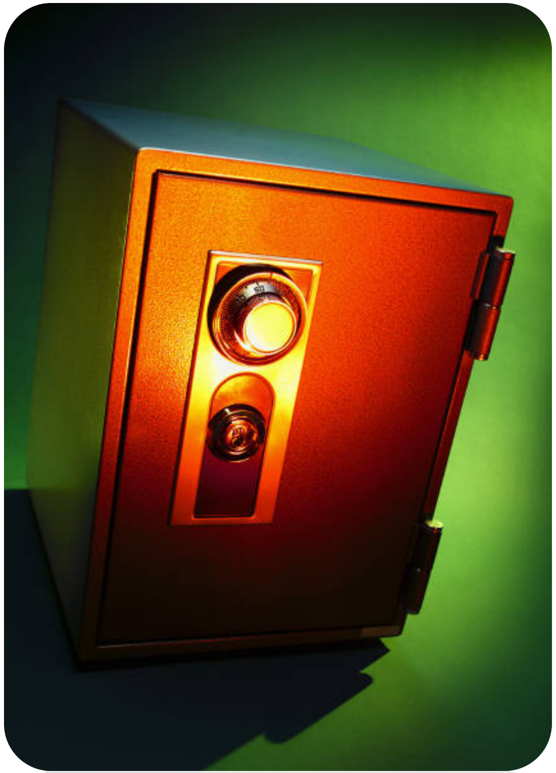
2. Thou Shall Not Text

- Why are members of the workforce texting?
- Is e-mail effective?
- Is a no-texting policy effective, or is secure texting needed?

# Identify Mobile App Needs

3. Thou Shall Not Place PHI on Thy Smartphone or Tablet

- Why is PHI ending up on smartphones?
- Is remote access to PHI sufficient?
- Is a secure vault for PHI needed?



# Identify Mobile App Needs

Patient Engagement

- Improved access to EHR (MU Stage 2)
- Ability to accept patient health information (e.g., iBlueButton)
- Improved treatment communications and adherence
- Appointment reminders

# Identify Mobile App Solutions

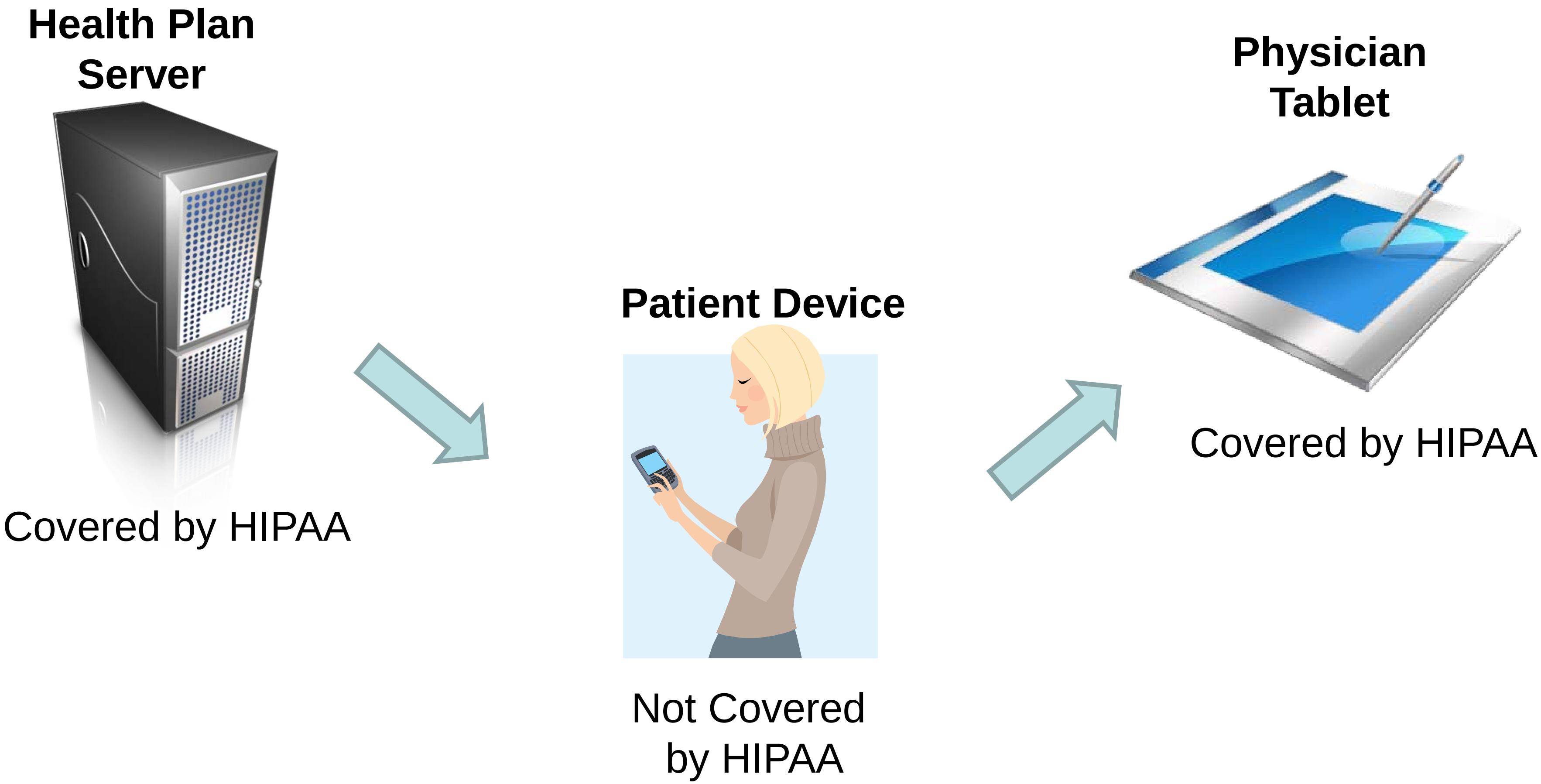
- Mobile diagnostic tools
- Secure access to e-mail
- Mobile EHR portal
- Secure texting
- Secure container
- Secure access to Blue Button data
- Remote wipe and antivirus

# Include Mobile Apps in Risk Analysis

**Identify where PHI is located on mobile devices**

- **C** - What apps Create PHI (e.g., diagnostic apps)
- **R** - What apps Receive PHI (e.g., EHR portal, e-mail, iBlueButton)
- **M** - What apps Maintain PHI (e.g., e-mail, secure container)
- **T** - What apps Transmit PHI (e.g., secure texting)

# HIPAA Hot Potato



**Health Plan Server**

Covered by HIPAA

**Patient Device**

Not Covered by HIPAA

**Physician Tablet**

Covered by HIPAA

# Include Mobile Apps in Risk Analysis

Identify threats and vulnerabilities

- What if mobile device is lost, stolen, or replaced?
- What if mobile device is shared?
- Can malware on device lead to unauthorized access?
- Can transmissions be intercepted by unauthorized third party?
- Is PHI on device reasonably available?

# Include Mobile Apps in Risk Analysis

Identify current security controls?

- Is information encrypted while maintained?
- Is information encrypted in transit?
- What authentication of app users is in place?
- Is PHI backed up when necessary?
- Can PHI be remotely wiped?

# Include Mobile Apps in Risk Analysis

Identify likelihood, impact, and aggregate risk

- What is the likelihood of a threat exploiting a vulnerability?
- What is the impact if exploited?
- Likelihood x Impact = Risk

# Implement Risk Management Strategy

- What risks are medium and high?
- Can risks be lowered to reasonable amounts through:
  - Policies
  - Training
  - Additional technical controls (e.g., locking down the device or adding remote wipe features)

# Obtain Necessary BAAs & Due Diligence

- Does the app developer create, receive, maintain, or transmit PHI on covered entity's behalf?
  - If PHI is encrypted and app developer does not have the key, HIPAA is unclear as to whether BAA is needed
- Due diligence - What is app developer's security?

# Document Security Rule Compliance

- ✓ Included in risk analysis
- ✓ Included in risk management
- ✓ Sanctions for violations of policy
- ✓ Reasonably review system activity
  - If activity cannot be centrally reviewed, document whether this is reasonable
- ✓ Authorization, supervision, and clearance
  - Who needs access to PHI on mobile devices

# Document Security Rule Compliance

- ✓ Termination procedures
  - Is PHI on mobile devices secured and access through apps terminated at employment termination
- ✓ Include mobile apps in security awareness and training
- ✓ Address potential malware on mobile device
- ✓ Address mobile app passwords

# Document Security Rule Compliance

- ✓ Identify and respond to mobile app security incidents
- ✓ Ensure that PHI in mobile apps is reasonably backed up
- ✓ Integrate mobile apps into contingency planning
- ✓ Evaluate mobile app program

# Document Security Rule Compliance

- ✓ Address physical security of mobile devices
- ✓ Address which mobile devices need to be inventoried
- ✓ Ensure proper disposal/re-use of mobile devices with apps containing PHI
- ✓ Address whether mobile devices need to be backed up

# Document Security Rule Compliance

- ✓ Address automatic logoff of mobile apps
- ✓ Address encryption of data maintained by apps on device
- ✓ Address encryption of data transmitted by mobile app
  - Document basis for transmission of some PHI without encryption

# PRIVACY RULE AND MOBILE APPS

# The X-Factor

# Right of Access

- Patient may access copy of designated record set in requested form and format, if readily producible
- Mobile app to portal may be convenient means of providing access (and support MU Stage 2 objectives)
- <u>But,</u> patient may prefer unencrypted e-mails (permissible after warning of risk)

# Right to Confidential Communications

- Must accommodate reasonable requests for communications to patient by alternative means or at alternative location
  - Some patients may prefer communications through unencrypted e-mails
  - Other patients may not want unencrypted appointment reminders

# Don’t Let Security Trump Patient Preference

## (No matter how much you paid for that secure mobile app)

# For more information…

**Adam H. Greene, JD, MPH**

Davis Wright Tremaine LLP

**adamgreene@dwt.com**
**202.973.4213**