mHealth Data Security - Lack of Standards for Synchronous Care

1. HIPAA consistent data security is required

2. We have more questions than answers

3. The following will address some of those questions, and propose discussion points
Current Standards

1. Standards for HIPAA consistent and good practices do exist
   a. Sessions should be secured to greatest practical extent through private, point-to-point, or a virtual private network (VPN)
   b. Network and software security protocols
   c. Accessibility and authentication protocols
   d. Safeguards against data storage and transmission corruption
What the Standards Must Accomplish

1. Interoperability among disparate systems
2. Future interoperability of legacy systems
3. Efficient storage and transmission of multi-media
4. Transparency to user
5. Security and integrity of “data at rest”, “data in use”, and “data in motion”
# Technical Security Options

<table>
<thead>
<tr>
<th>OPTION</th>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
</table>
| Web server       | • Standards for transmission exist  
                   • Data on secure server, not device | • Lack of native functionality  
                   • Dependent on server access |
| Mobile framework | • Standardization between applications and OS  
                   • Not dependent on OS | • Costs for test and development  
                   • Different platforms |
| Operating System | • Standards built-in  
                   • Shared costs  
                   • Partnerships | • Different OS companies  
                   • Complexity for common standards |
| Combination      | • Strengths of each option  
                   • Partnerships  
                   • Standardized across platforms | • Time consuming to build  
                   • Dependencies |

## Authentication Options

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>METHODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Something Known</td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• Personal Identification Number</td>
</tr>
<tr>
<td></td>
<td>• Pass Phrase</td>
</tr>
<tr>
<td>Something Possessed</td>
<td>• Mobile Device Identification Number</td>
</tr>
<tr>
<td></td>
<td>• Tokens (USB, key fob, etc)</td>
</tr>
<tr>
<td></td>
<td>• Dongle</td>
</tr>
<tr>
<td></td>
<td>• Smart Card</td>
</tr>
<tr>
<td></td>
<td>• Radiofrequency Identification</td>
</tr>
<tr>
<td>Something Unique to the Person</td>
<td>• Fingerprints</td>
</tr>
<tr>
<td></td>
<td>• Iris Scan</td>
</tr>
<tr>
<td></td>
<td>• Retina Scan</td>
</tr>
<tr>
<td></td>
<td>• Voice Print</td>
</tr>
</tbody>
</table>

Concluding Statements

1. Stepped approach best for flexible development
2. Issue focuses too much on “written” rather than technical and hardware standards
3. Standardization will require partnerships between consumers, industry, advocates, and governments
Reimbursement - Some Questions?

1. Where is care delivered?
2. Is it medical care?
3. What is the transmission speed? Screen size? Other technical specs?
4. What is coded for the session or assessment?
5. How was data secured?
6. Who is responsible?
7. Who is present?
Favorite FDA mHealth Myths

Saturday, April 28, 2012

Dane Stout
Executive Director
Connected Health Practice
Anson Group LLC
CHOOSE YOUR PERSONAL FAVORITE

1. **MYTH:** We’re a just a _______(software, platform, telco, handset, video conferencing, consumer electronics, etc.) company and FDA doesn’t regulate us.
2. **MYTH:** We are a health care delivery institution and FDA doesn’t regulate the practice of medicine.

3. We’ve been selling our products for years and FDA has never bothered to contact us, which I guess means we’re not regulated.
4. **MYTH: FDA doesn’t regulate HIT software, only medical devices.** My product is HIT software.

5. **MYTH: FDA should be fine with us; our products have MU certification from an authorized testing authority and are HIPAA compliant.** We even have a grant money from CMS/ONC/NIH/VA (etc.) for our innovation. meets the HIPAA definition of personal health information.
6. **MYTH:** Our product is HIPAA certified, or we use only HIPAA certified products in our facility, so we’re OK.

7. **MYTH:** Our company isn’t a physician, healthcare provider facility, or insurance company, and therefore isn’t subject to HIPAA regulation.

8. **MYTH:** As long as we encrypt our data during transmission we’ll be OK.
9. **MYTH:** We have submitted our product to FDA and received premarket clearance to sell it, so time to start selling to insurers and CMS.

10. **MYTH:** I’ll submit my data to CMS first, and then the private payers will pick it up as long as I can convince Medicare and Medicaid to pay for it.
OTHER MISCONCEPTIONS

??????????s

COMMENTS
PANELISTS and MODERATOR

Bradley Merrill Thompson, JD, EpsteinBeckerGreen, bthompson@ebglaw.com
Matt C. Mishkind, PhD, National Center for Telehealth and Technology (T2), matt.mishkind@us.army.mil
Dane Stout, Anson Group LLC, dstout@ansongroup.com
Napoleon Monroe, New Directions Technology Consulting, LLC. nap.monroe@newdirectionsconsulting.net
Regulatory, Privacy/Security and Reimbursement Issues

Saturday, April 28, 2012

Moderator: Napoleon Monroe
New Directions Technology Consulting, LLC
INTRODUCTION

The regulator’s mission is to protect the public health. Devices (including software) must be safe and effective.

Privacy, security and reimbursement are woven into the regulatory requirements.

So is risk management.
INTRODUCTION

Regulatory concerns aside, privacy/security, managing risk and being paid are essential to building a business.

mHealth cannot be successfully integrated unless we address regulatory issues including privacy/security, reimbursement and risk management.
INTRODUCTION
Approaches to all these areas are works in progress. There are few clear-cut rules. We’ll share some experiences and learn from your questions.

Hopefully this session will help all of us define how to address these issues.
PANELISTS
Bradley Merrill Thompson, JD, Member of the Firm, EpsteinBeckerGreen, Washington, DC
Matt C. Mishkind, PhD, Research Psychologist/Program Lead, Clinical Telehealth Division, National Center for Telehealth and Technology (T2), Tacoma, WA
Dane Stout, Executive Director, Connected Health Practice, Anson Group LLC, Indianapolis, IN
FDA Regulation of mHealth

Saturday, April 28, 2012

Bradley Merrill Thompson
Epstein, Becker & Green P.C.
1. Fundamentals of Device Regulation
2. FDA Regulation of mHealth
   a. Medical Device Data Systems
   b. Mobile Medical Apps
   c. Clinical Decision Support Software
3. MRC Policy Development
Device Definition Distilled

To be a device, boiled down to its essence, there are two criteria:

1. A physical product is involved and
2. The product is “intended” for a medical use, including use as accessory to a medical device.
FDA’s Accessory “Rule”

FDA can also regulate accessories to a medical device

– An accessory is a finished medical device that is sold as an addition to another finished medical device to augment or supplement its performance.

– Accessories are regulated at the same classification as the finished medical device.

  • Unless the accessory is itself classified, like MDDS
Medical Device Data Systems

- Storage
- Conversion
- Display
- Transfer

Medical Device Data

- Active Patient Monitoring
- Control Connected Medical Device
- Modify
- Analyze
Mobile Medical Apps (MMA) Guidance

Medical Device Intended Use

- Accessory to a Regulated Device

OR

- Transforms a Mobile Platform

= Mobile Medical App

### MMA

- “Connect to” one or more medical device(s)
- Transform the mobile platform
- Output a patient-specific result

### Not an MMA

- Electronic medical textbooks
- Training tools or generic aids
- General health and wellness
- Automate general office operations
- Electronic health record

### Unclear

- Automate common medical knowledge
- Tool for self-management of disease
- Automate common diagnostic/treatment tasks
Clinical Decision Support Software

Preliminary Definition

**Information**
- Data from a medical device
- Environmental data (e.g., pollen count, temp.)
- Demographic data (e.g., age, sex, socio-economic status)

**Conversion**
- Algorithms (fixed or iterative)
- Formulae
- Database look-ups or comparisons
- Rules or associations

**Clinical Decision**
- Patient-specific
- Actionable result
mHealth Regulatory Coalition (MRC)

What will FDA regulate?

In what device class?
MRC Proposed Guidance

Intended Use Claims

Software Apps

Accessories & Claims of Compatibility
Intended Use Claims

Within FDA Jurisdiction

Medical Devices

- Disease related claims that **clearly** constitute device claims.

Uncertain Jurisdiction

A. Socially Beneficial, Low Risk Devices

- Wellness related claims that **could** constitute device claims, but **should not be regulated** to encourage development.

B. Ambiguously Defined, Low Risk Products

- Disease/wellness related claims that **might** constitute device claims, but it is **unclear**.

Outside FDA Jurisdiction

Consumer Products

- Wellness related claims that **clearly do not** constitute device claims.
Sample of Health-Related Apps in iTunes

- Reg. Device: 56%
- SBLR: 19%
- ADLR: 17%
- Unreg. Product: 8%
Regulation of Accessories

Create an independent classification applicable to the accessory

Require claims of compatibility to be substantiated by the claim maker
Accessory Classifications

- Physical Therapy App
- Sleep Monitoring App
- Stress Mgmt. App
- MDDS
- Weight Mgmt. App
- Diabetes App
- Cardiac Disease App
- Therapy Compliance App
- Activity Monitoring App
- Class I Controller App
- Class II/III Controller App
- General Aggregator App
- Diabetes Aggregator App
- Cardiac Aggregator App
- Therapy Aggregator App
- Activity Aggregator App
Software Modularization

Use of standard design principles creates functional independence and reduces inherent risk of discrete modules.