The Age of Healthcare Consumerisation:

Wearables, Health Apps, Remote Patient Monitoring and Health Data

Presented By:
Ryan P. Blaney, Esq.
Washington, DC
rblaney@cozen.com
Agenda

• “Uberification” of Healthcare
  – The Healthcare Internet of Things (IoT)

• Regulatory Guidance and Trends

• Unique Privacy & Security Concerns in the Age of Healthcare Consumerisation

• Privacy Considerations for International Companies Investing and Doing Business with U.S. Healthcare Companies
Uberification of Healthcare

- Uber’s Goal – “to make transportation of people easier and more efficient.”
- On Demand Mobile Services (ODMS)
- “Making getting care easier”
  1. Big Data and Personalized Medicine
  2. Telemedicine
  3. Remote Patient Monitoring
  4. Healthcare Apps
Big Data and Personalized Medicine

“[Genome Science] will revolutionize the diagnosis, prevention and treatment of most, if not all, human diseases.”

Do you know when and who???
June 26, 2000 – First Survey of Human Genome
Predictive Analytics

“Figuring out how to get the right drug, to the right person, at the right dose, at the right time.”

Dr. Francis Collins
National Institute of Health
What is Predictive Analytics?

• Predictive analytics is the process of learning from historical data in order to make predictions about the future (or any unknown)

• For healthcare, predictive analytics will enable the best decisions to be made, allowing for care to be personalized to each individual
Big Data in Healthcare – Why Now?

Source: American Informatics Association

<table>
<thead>
<tr>
<th>Year</th>
<th>Petabytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>500</td>
</tr>
<tr>
<td>2020</td>
<td>25000</td>
</tr>
</tbody>
</table>
Big Money

• $1.9 Billion into companies that purported to use predictive analytics.

Source: Rock Health Funding Database
New Data Streams

“Current data sets generally revolve around claims but that’s going to be changing with lots of clinical data and transactional information with lifestyle becoming more readily accessible.”

Dr. Same Ho – Chief Medical Officer, United Healthcare
Uberification: Telemedicine

Either you have a new virus or my computer does.
Uberification: Remote Patient Monitoring

• RPM - is a technology to enable monitoring of patients outside of conventional clinical settings (e.g. in the home), which may increase access to care and decrease healthcare delivery costs.
Uberification: Healthcare APPs

• Pharmaceutical apps
• Provider Apps
• Payor Apps

“As mobile apps continue to grow in popularity, a question arises of how patients can be confident they’re downloading safe, effective apps.”
FDA Mobile Health Guidance

FDA’s Mission:

“Protecting the public health by assuring the safety, effectiveness and security of .... Medical devices.”

Why the FDA is looking at digital health?
Scope of FDA Oversight

Draft Guidance for Industry and Food and Drug Administration Staff

Mobile Medical Applications

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Document issued on: July 21, 2011

You should submit comments and suggestions regarding this draft document within 90 days of publication in the Federal Register of the notice announcing the availability of the draft guidance. Submit written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Submit electronic comments to http://www.regulations.gov. Identify all comments with the docket number listed in the notice of availability that publishes in the Federal Register.

For questions regarding this document, contact Bakul Patel at 301-796-5528 or by electronic mail at Bakul.Patel@fda.hhs.gov. For questions regarding this document concerning devices regulated by CBER, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 301-427-1860.

U.S. Department of Health and Human Services
Food and Drug Administration

Center for Devices and Radiological Health

Center for Biologics Evaluation and Research
Definition of Medical Device

• An instrument, apparatus, implement, machine, contrivance, implant, or in vitro reagent that is intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease in man, or intended to affect the structure or any function of the body.
Is this a Mobile Medical App?

• Key question: Is your app’s intended use (alone or in concert with a device – regulated or otherwise) to diagnose, treat, mitigate, cure, or prevent a specific disease or condition?
Uberification: Wearables

• Market is expected to grow over the next 10 years from $14 billion to $70 billion.
• “We are taking a very light touch, an almost hands-off approach,” FDA’s associate director for digital health.
• The Apple Effect????
  – Partnerships with major health care providers – Mayo Clinic
  – Epic’s Electronic Medical Records
Wearables: Healthcare Payors

• Company health plans: 94% of consumers currently enrolled in wellness programs familiar with Apple Watch

• Health Insurance company Oscar teamed up with wearable device maker, Misfit to offer free activity trackers for all uses and offer rewards for being active.
Wearables: Life Insurance

• Discovery - International life and disability policies
• Vitality – based in South Africa
• According to a New York Times article published on April 8, 2015 – “John Hancock will become the first life insurance company to introduce a similar program for American consumers.”
The Future of Wearables
US, EU and International Regulations
Who is the Enforcer in the US?
Mobile Health; Consumers
The Feds Training the AGs
State Attorney General Enforcement

- State Attorney Generals have started to exercise the authority granted by HITECH to bring civil actions on behalf of state residents for violations of HIPAA
- Connecticut, Vermont, Massachusetts, Minnesota AGs have brought actions under HIPAA
  - Minnesota went against a BA
Andrew Paterson’s Blog Entry

- Wearable technology must comply with UK data privacy laws
ICO – Requirements

- Organizations collecting information through wearables must:
  1. Inform people how their data is being collected and used
  2. Only collect information that is relevant, adequate and not excessive
  3. Comply with CCTV Code of Practice
  4. Keep the Information Secure
  5. Delete it once it is no longer required
Australian Privacy Commissioner

- Encouraged organizations to develop policies for the use of wearable technologies at work.
Published research report, “Wearable Computing: challenges and opportunities”

Personal Information Protection and Electronic Documents Act (PIPEDA)

“wearable devices can amplify privacy risks …”
Unique Privacy & Security Concerns in the Age of Healthcare Consumerisation
Privacy Concerns for Wearables

1. Can your data be shared with or sold to third parties?
2. What measures will the company or third party vendors take to ensure that PHI and non-covered PHI is safe and secure?
3. What are the default privacy settings? Are they set to public or private?
4. Health Data is not necessarily protected by HIPAA
5. Who Owns the Data?
Privacy Issues for Wearables

• Company bring your own device (BYOD) issues
• Voice recordings and labor and employment issues
• Need to update company privacy policies for wearable technologies
• Technology is coming very fast … the law needs to keep up
Non-Healthcare International Companies

- Privacy Considerations for Companies Investing and Doing Business with U.S. Healthcare Companies
What is HIPAA?

• The Health Insurance Portability And Accountability Act of 1996 (HIPAA)
  – Administrative Simplification
    • Standards for health care electronic transactions and code sets
    • Security of electronically stored and transmitted health information.
    • Privacy of individually identifiable health information
What is HIPAA?

• **Privacy Rule** – sets the standards for who may have access to PHI
  – applies to all forms of PHI whether electronic, written or oral

• **Security Rule** – sets the standards for ensuring that only those who should have access to electronic PHI (E PHI) will actually have access
  – Only applies to PHI that is in electronic form
HIPAA Applicability

• Covered Entities
  – **Health plans** - including, for example:
    • Group Health Plans (medical, dental and LTC plans)
    • Health insurance issuers
    • Issuers of Flexible spending accounts
  – **Health care providers** that transmit electronic information in connection with health claims transactions
  – **Health care clearinghouses**
HIPAA Applicability

• Business Associates
  – a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information
  – Examples include billing companies, attorneys, accountants, consultants, etc.
HIPAA General Rule

• PHI may not be disclosed without patient authorization unless the disclosure is otherwise permitted by HIPAA or required by law.

• Failure to comply = breach
  – Breach notification if unsecured PHI
Top HIPAA Issues - Breach

• Revised Definition of “Breach:”
  – Breach presumed unless:
    • “LoProCo:” The CE or BA can demonstrate that there is a low probability that the PHI has been compromised based on:
      – Nature and extent of the PHI involved (including the types of identifiers and the likelihood of re-identification;
      – The unauthorized person who used the PHI or to whom the disclosure was made;
      – Whether the PHI was actually acquired or viewed; and
      – The extent to which the risk to the PHI has been mitigated.
  – Focus on the risk to the data, instead of risk of harm to the individual
"I heard the new HIPAA Omnibus Rules are a whole lot tougher on business associates."
500+ Breaches by Type (%)
500+ Breach by Location of PHI (%)

- Laptop: 22
- Desktop: 13
- Paper: 12
- Other: 11
- EMR: 6
- Email: 4
- Network Server: 6
- Portable Device: 21

COZEN O'CONNOR
Lessons Learned

• Appropriate Safeguards can prevent breaches:
  – Evaluate the risk to e-PHI when at rest on removable media, mobile devices and computer hard drives
  – Take reasonable and appropriate measures to safeguard e-PHI
  – Encrypt data stored on portable/moveable devices & media
  – Consider appropriate data backup
  – Train workforce members on how to effectively safeguard data and report security incidents.
Lessons Learned from Enforcement

• HIPAA CEs and BAs are required to undertake a careful risk analysis
  – understand the threats and vulnerabilities to individuals’ data
  – have appropriate safeguards in place to protect this information.

• Take caution when implementing changes to information systems.

• Create a “Culture of Compliance”

• CMPs
"Oh, that’s for security. We all keep our user name and password on a sticky note hidden where it’s safe."
Employ Strong, Unique Passwords

- Passwords are like underwear:
  - You shouldn’t leave them out where people can see them
  - You should change them regularly
  - You shouldn’t loan them out to others

- Strong passwords: 8+ characters long with upper/lower characters, numbers, and symbols that don’t contain your user name, real name, or company name

- Unique passwords: No two passwords are exactly the same – use a password convention
Use Two-factor Authentication

- **Two** Factors:
  - Something you know
  - Something you possess

- Use with:
  - Personal email accounts
  - Device accounts (e.g., Apple and Microsoft)
  - Financial intermediaries (where available)
    - Banks
    - Investment accounts
    - Credit cards
Hacking Defenses
Learn to Spot Phishing Messages

1. Is the email coming from the address you would expect?
2. Is there anything unusual about the message itself?
3. Is the message missing something you would normally expect to see?
4. Do the links point to what seem to be legitimate web pages?

PS - Did the message come to you as a surprise?
PPS - Do the message headers and IP addresses check out? (Ask IS.)

Use your smartphone to click a link if you absolutely must
Protect Your Home Computer

• Anti-virus/anti-malware
  – Current, real-time protection
• Firewall: Turn it on!
• Home router
  – WPA2
  – Change default passwords
• Clean-up (CCleaner)
• Backup/Restore capabilities
  – Online (Carbonite, CrashPlan)
  – External drive ($65 for 1TB)
  – Recovery USB flash drive
Recognize Signs of Common Scams

- A cold-call representative of a (non-US) company wants your help settling a litigation debt with a US business, needs local counsel, etc. **BUT:**
  - The caller doesn’t want to talk on the phone
  - The caller’s email address doesn’t match the companies domain (e.g, www.rbs.com v. mharris@rbsbank.com)
  - The email domain was registered recently (IS can make that determination)
  - Messages seem odd or unprofessional (capitalization, spelling, usage, signature lines)
  - The caller doesn’t show up in LinkedIn or public records searches
Watch Over Your Financial Accounts

- Set up email or text alerts for:
  - Credit card purchases
  - Debit card transactions
  - Bank account withdrawals or transfers
  - Investment account trades or transfers
- Check your credit report several times per year: Equifax, Experian, TransUnion
- Consider credit monitoring (despite mixed reviews?)
- Set up fraud alerts:
- Set up credit freezes if you’re high risk, divorcing, or need little to no credit
Thank You

Presented By:

Ryan P. Blaney, Esq.
Washington, DC
rblaney@cozen.com

Blog Co-Editor: Healthlaw Informer at:
http://www.healthlawinformer.com/