Investment in Telehealth

Ryan S. Higgins | April 6, 2016
Telehealth Market

- Globally, the telemedicine technologies market is predicted to grow to $34 billion in 2020. (Mordor Intelligence, 2015)
- Domestically, annual investment in “on-demand” health services will quadruple from $250 million to $1 billion by 2017. (Accenture, 2015)
- While the U.S. telemedicine market is the largest, international telemedicine programs are also growing at a significant pace, particularly in Europe and Asia. (Research and Markets, 2015)
- At a minimum, these reports evidence that telemedicine is not a passing phase but is here to stay both domestically and internationally.
Current Products and Services Segmentation

- 12% Medical education
- 13% Exchange of medical and health information
- 35% Remote patient monitoring and follow-up
- 40% Transmission of medical data and images for diagnosis

SOURCE: WWW.IBISWORLD.COM
Potential Drivers of Telehealth Investment

- Advances in communication technology and medical technology have propelled the industry forward.
- Aging population more likely to require health care.
- Advanced in medical technology, such as wearable devices, have created new opportunities for telemedicine.
- Increasing private insurance coverage of telehealth services will lead to increased industry revenue.

Key External Drivers
- Private investment in computers and software
- Number of adults aged 65 and older
- Federal funding for Medicare and Medicaid
- Demand from medical device manufacturing
- Number of people with private health insurance
- Prime rate

SOURCE: WWW.IBISWORLD.COM
Potential Deterrents to Investment

- Early Organizational and Compliance Costs
  - Corporate practice of medicine considerations (state by state)
  - Professional licensure considerations (state by state)
  - Reimbursement considerations (state by state)
  - FDA / medical device considerations (federal; compliance costs)
  - Data privacy and security considerations (state and federal; compliance costs)

- Avoid the pitfall of embracing status as a technology company to the exclusion of acknowledging dual status as a health care company.
Potential Deterrents to Investment: FDA / Medical Device Considerations

Although guidance documents are officially non-binding, they effectively set agency policy.
Potential Deterrents to Investment: FDA / Medical Device Considerations

“An instrument, apparatus, implement, machine . . . including any component, part or accessory. . .”

“intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease”

is a medical device
Potential Deterrents to Investment: FDA / Medical Device Considerations

- Manufacturer must intend that the product be used in diagnosis, treatment, etc., to be a medical device
- “Intended use” = the objective intent of the persons legally responsible for labeling the device
  - May be shown by expressions or by the circumstances surrounding the distribution of the product

The intended use of a mobile app determines if it meets the definition of a medical device.
## Potential Deterrents to Investment: FDA / Medical Device Considerations

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Is a product with this functionality a device?</th>
</tr>
</thead>
<tbody>
<tr>
<td>App that turns a phone into a flashlight</td>
<td>No</td>
</tr>
<tr>
<td>App that turns a phone into a flashlight to help doctors examine patients</td>
<td>Yes</td>
</tr>
<tr>
<td>App that generates reminders for scheduled appointments</td>
<td>No</td>
</tr>
<tr>
<td>App that controls an insulin pump</td>
<td>Yes</td>
</tr>
<tr>
<td>App that analyzes skin lesion and provides user with assessment of risk</td>
<td>Yes</td>
</tr>
<tr>
<td>Portal that matches patients with clinical trials</td>
<td>No</td>
</tr>
<tr>
<td>Medical journal</td>
<td>No</td>
</tr>
</tbody>
</table>
Potential Deterrents to Investment: FDA / Medical Device Considerations

- Notice of inspectional observations
- Warning letters, untitled letters
- Adverse publicity, seizures, injunctions
- Recalls (removals, corrections)
- Consent decrees, detention, refusal of entry
- Criminal charges, civil claims
- Monetary penalties, disqualification of clinical investigators
Potential Deterrents to Investment: Data Privacy and Security Considerations

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Amended by the Health Information Technology for Economic and Clinical Health Act (HITECH)

- Other Federal Laws
  - Federal Alcohol and Drug Abuse Confidentiality Law
  - Children’s Online Privacy Protection Act (COPPA)
  - Genetic Information Non-Discrimination Act (GINA)
  - Federal Trade Commission Act (FTC)
  - Gramm-Leach-Bliley Act (GLBA)
  - Fair Credit Reporting Act (FCRA)
  - Telephone Consumer Protection Act (TCPA)

- State Laws
  - Constitutional Right of Privacy
  - State statutes and regulations protecting confidentiality of general health information
  - State statutes and regulations protecting confidentiality of sensitive categories of personal health information (e.g., HIV/AIDS, Mental/Behavioral Health, Substance Abuse, Genetic Testing/Counseling)
  - State Data Breach Notification Laws
  - State Data Disposal Laws
  - State Consumer Protection Laws
  - Common Law Case Law

- Industry Standards
  - Payment Card Industry Security Standards Council
  - Mobile Medical Marketing Association
  - National Telecommunications and Information Administration
Example of Potential Deterrent to Investment: Data Privacy and Security

- Federal and State Privacy and Security Laws Often Depend on:
  - The *type of information* collected, for example
    - GINA applies to genetic information in the context of employment and insurance
    - HIPAA applies to health information in certain contexts
    - State breach laws frequently cover SSNs, financial account numbers, etc.
  - The *type of individual* about whom the information is collected
    - COPPA applies to an “operator of a website or online service” that collects any “personal information” from children or is “directed to children”
  - The *type of industry or commercial sector* being regulated
    - GLBA applies to financial institutions
    - HIPAA applies to certain health industry related entities or individuals
Potential Deterrents to Investment: Data Privacy and Security Considerations

- Telehealth companies that lack a robust privacy and security infrastructure may present a risk to investors
  - Telemedicine providers have the same obligations to safeguard patient health information as providers who provide in-person care
  - The telemedicine provider must store electronic files, images, and audio or video files in a secure way
  - The storage and transmission of patient information between the telemedicine provider, the patient and/or other providers must be done in a secure manner, and comply with applicable state and federal laws and regulations
Potential Deterrents to Investment: Data Privacy and Security Considerations

- HIPAA specific considerations:
  - Must conduct a comprehensive security risk assessment
  - Must implement written privacy and security policies and procedures satisfying HIPAA requirements
  - Must notify certain third parties in the event of a “breach” of unsecured protected health information
  - Civil monetary penalties:
    - Unknowing ($100 per violation / $1.5M max)
    - Reasonable Cause ($1K per violation / $1.5M max)
    - Willful neglect ($10K per violation / $1.5M max)
    - Uncorrected willful neglect ($50K per violation / $1.5M max)
Thank you for your participation!

Ryan S. Higgins  
Partner, McDermott Will & Emery LLP  
(312) 984-2052  
rshiggins@mwe.com
Investment in Telehealth

Ryan S. Higgins | April 6, 2016

Illinois Telehealth Law Forum Series