Ray's Retreat 2017

A Model for IP Considerations

Raymond A. Miller
N. Nicole Stakleff
Barry H. Boise
Joseph Helmsen (in absentia)

Pepper Hamilton LLP
Attorneys at Law

August 9, 2017

Innovation without protection is philanthropy

-Mark Blaxill & Rick Eckardt, The Invisible Edge

Pepper Hamilton LLP
Attorneys at Law

Inter-related Nature of IP and Data

Pepper Hamilton LLP
Attorneys at Law

Protection Process

- Capturing IP internally
  - Think broadly, holistically
  - Anticipate future trends (e.g. use of big data / AI in clinical trial evaluation/reporting, responder analysis, reimbursement, post-market surveillance)
  - Educate and communicate with employees & advisors
- Collaborate externally
- Monitor competitors
- “Make Deal-Readiness a Daily Discipline” - Andrew Powell
  - Best practices for contracts and licensing, employees
  - Maintain organized IP database
  - IP due diligence mode / contemplate reps & warranties
  - Conduct regular internal audits

- U.S. Food and Drug Administration

Hypo

Gash Inc. is a wound care company that provides a range of prescription and nonprescription wound care products, including ointments, creams, bandages and sutures.

App designer pitches marketing group with an exciting new idea called the “Wound Warlock” App with a range of functionality.

Hypo

App uses camera on phone or tablet, and helps asses the healing of a wound.

The Wound Warlock saves patient and doctor time, and may improve patient outcomes by linking to Gash products that will tie to the patient need.

What is a Medical Device?

An instrument, apparatus, implement, machine, contrivance, or other similar or related article, including a component part or accessory, that is intended:

- for use in the diagnosis of disease or other conditions;
- for use in the cure, mitigation, treatment, or prevention of disease; or
- to affect the structure or any function of the body

Source: 21 U.S.C. §321(h)

February 9, 2015, FDA Guidance on Mobile Medical Applications

- What is the force of a “Guidance”?
- FDA intends to regulate mobile medical software that poses a threat to public safety
- The key regulatory factor is the intended use of the mobile health application
- Mobile medical Apps will be subject to the same standards FDA applies to traditional medical devices

Glooko glucose monitoring logbook app and cable, © 2015 Glooko, Inc.

Pepper Hamilton LLP
Attorneys at Law

FDA Will Regulate:

- Extending medical device **to control** the device for use in active patient monitoring
- Acting as an **accessory** to a medical device
- Using attachments, screens, sensors to **transform** mobile platform into a medical device
- Performing **patient-specific** analysis
- Assisting with diagnosis or **patient-specific** treatment recommendations

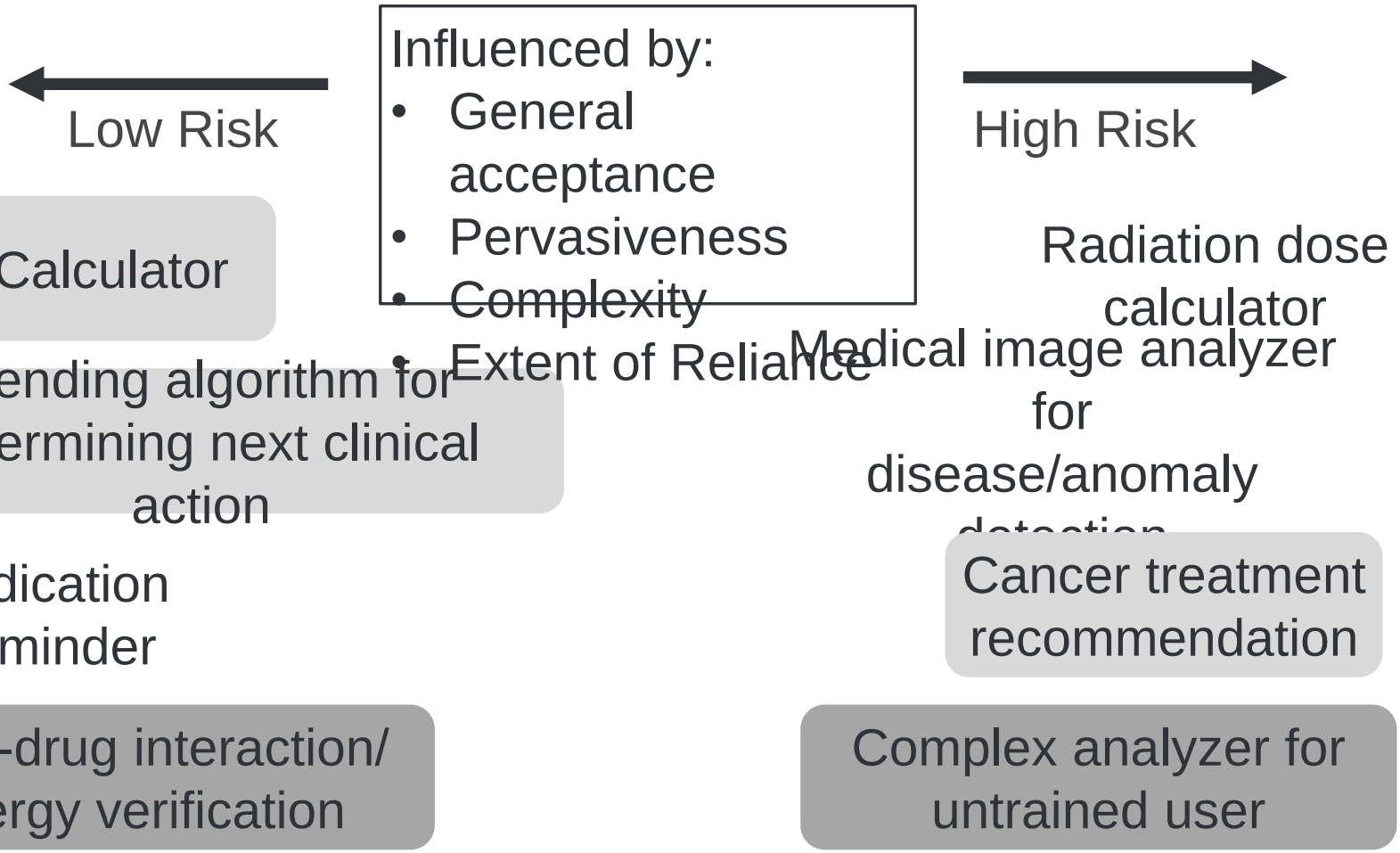
Source: February 9, 2015, FDA Guidance on Mobile Medical Applications

FDA Does Not Intend to Regulate:

- Providing patients with tools to organize/track health information
- Helping patients document or communicate medical information to providers or access Medical Records
- Performing **simple** calculations used in clinical practice
- Enabling individuals to interact with EHRs and PHRs

Source: February 9, 2015, FDA Guidance on Mobile Medical Applications

Understanding Risk



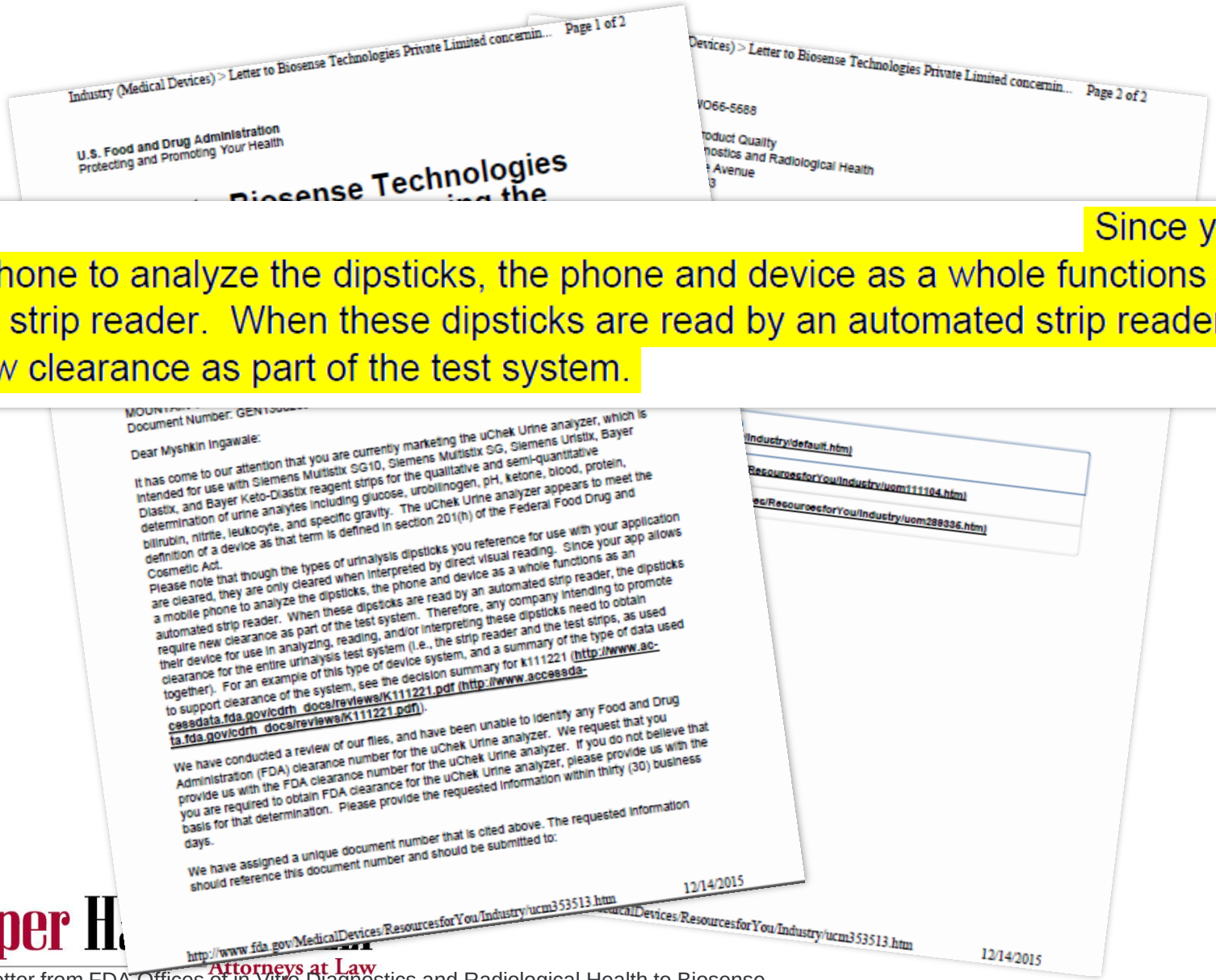
Example of an FDA-Regulated Accessory

uChek app allowed users to analyze their urinalysis dipsticks using the camera on their mobile phone

- Dipstick is a cleared Medical Device approved only for direct visual reading
- App now enables a mobile phone to analyze the dipstick

Source: May 2013 Letter from FDA Offices of in Vitro Diagnostics and Radiological Health to Biosense

Approved Device Analyzed by App Requires New FDA Clearance



Since your app allows a mobile phone to analyze the dipsticks, the phone and device as a whole functions as an automated strip reader. When these dipsticks are read by an automated strip reader, the dipsticks require new clearance as part of the test system.

Industry (Medical Devices) > Letter to Biosense Technologies Private Limited concernin... Page 1 of 2

U.S. Food and Drug Administration
Protecting and Promoting Your Health

Biosense Technologies

Devices) > Letter to Biosense Technologies Private Limited concernin... Page 2 of 2

Document Number: GEN

Dear Myshkin Ingawale:

It has come to our attention that you are currently marketing the uChek Urine analyzer, which is intended for use with Siemens Multistix SG10, Siemens Multistix SG, Siemens Uristix, Bayer Diastix, and Bayer Keto-Diastix reagent strips for the qualitative and semi-quantitative determination of urine analytes including glucose, urobilinogen, pH, ketone, blood, protein, bilirubin, nitrite, leukocyte, and specific gravity. The uChek Urine analyzer appears to meet the definition of a device as that term is defined in section 201(h) of the Federal Food Drug and Cosmetic Act.

Please note that though the types of urinalysis dipsticks you reference for use with your application are cleared, they are only cleared when interpreted by direct visual reading. Since your app allows a mobile phone to analyze the dipsticks, the phone and device as a whole functions as an automated strip reader. When these dipsticks are read by an automated strip reader, the dipsticks require new clearance as part of the test system. Therefore, any company intending to promote their device for use in analyzing, reading, and/or interpreting these dipsticks need to obtain clearance for the entire urinalysis test system (i.e., the strip reader and the test strips, as used together). For an example of this type of device system, and a summary of the type of data used to support clearance of the system, see the decision summary for k111221 (http://www.accessdata.fda.gov/cdrh_docs/reviews/K111221.pdf (http://www.accessdata.fda.gov/cdrh_docs/reviews/K111221.pdf)).

We have conducted a review of our files, and have been unable to identify any Food and Drug Administration (FDA) clearance number for the uChek Urine analyzer. We request that you provide us with the FDA clearance number for the uChek Urine analyzer. If you do not believe that you are required to obtain FDA clearance for the uChek Urine analyzer, please provide us with the basis for that determination. Please provide the requested information within thirty (30) business days.

We have assigned a unique document number that is cited above. The requested information should reference this document number and should be submitted to:

http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm353513.htm 12/14/2015

/Industry/default.html

ResourcesforYou/Industry/ucm111104.html

es/ResourcesforYou/Industry/ucm288336.html

http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm353513.htm 12/14/2015

Pepper Ha

Attorneys at Law

Source: May 2013 Letter from FDA Offices of In Vitro Diagnostics and Radiological Health to Biosense

What about Regulation SaMD?

- FDA acknowledges current regime not appropriate
- FDA (Draft) Guidance based on IMDRF
  - Harmonize quality of evidence
    - Analytical, Scientific, Clinical Validity
  - Function
    - Inform
    - Directing Decision-Making
    - Diagnoses or Treatment
  - Seriousness of Disease
- Pilot Program announced August 1, 2017
- Designed to inform regulatory status of Clinical Decision Software guidance

Pepper Hamilton LLP
Attorneys at Law

FDA and Cybersecurity

Premarket Cybersecurity

- On October 2, 2014, the FDA released a Guidance regarding the management of cybersecurity risks in the design and development of interconnected medical devices.
- Adopted the National Institute of Standards and Technology's proposed cybersecurity framework:
  - Limit access to trusted users
  - Ensure trusted content; and
  - Detect, respond, and recover
- Recommend submission of cybersecurity control information in premarket submissions.

Source: FDA, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (Oct. 2, 2014), available at http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

FDA and Cybersecurity

Postmarket Cybersecurity

- On January 22, 2016, the FDA announced draft guidance identifying steps manufacturers should take to identify and address postmarket cybersecurity vulnerabilities that pose a risk to patient safety and public health.
- FDA recommends adoption of risk management program to monitor, identify, detect, assess, and mitigate cybersecurity vulnerabilities arising postmarket.
- "Uncontrolled" risks (posing an unacceptable risk that the clinical performance of a device could be compromised) may result in reporting obligations.

Source: FDA Draft Guidance, "Premarket Management of Cybersecurity in Medical Devices" (Jan. 22, 2016), available at http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

- Federal Trade Commission Enforcement

Start with Security

The FTC provided guidance from lessons learned from 50+ data security-related enforcement actions

1. Start with security
2. Control access to data sensibly
3. Require secure passwords and authentication
4. Store sensitive personal information securely and protect it during transmission
5. Segment your network and monitor who is trying to get in and out
6. Secure remote access to your network
7. Apply sound security practices when developing new products
8. Make sure your service providers implement reasonable security standards
9. Put procedures in place to keep your security current and address vulnerabilities that may arise
10. Secure paper, physical media and devices

FTC Best Practices for Mobile Health App Developers

- Minimize data
- Limit access and permissions
- Keep authentication in mind
- Consider the mobile ecosystem
- Implement security by design
- Don’t reinvent the wheel
- Innovate how you communicate with users
- Don’t forget about other applicable laws

Mobile Health Applications and HIPAA

- On October 5, 2015 the U.S. Department of Health and Human Services Office for Civil Rights (OCR) released an online platform for mobile application developers and others to submit questions and comments to anonymously to OCR on HIPAA compliance issues.
- OCR posted health application use scenarios in in February, 2016 to help provide clarity as to the application of HIPAA to use of mobile applications in certain situations.
- April 2016, Joint Guidance – Mobile Health Apps Interactive Tool

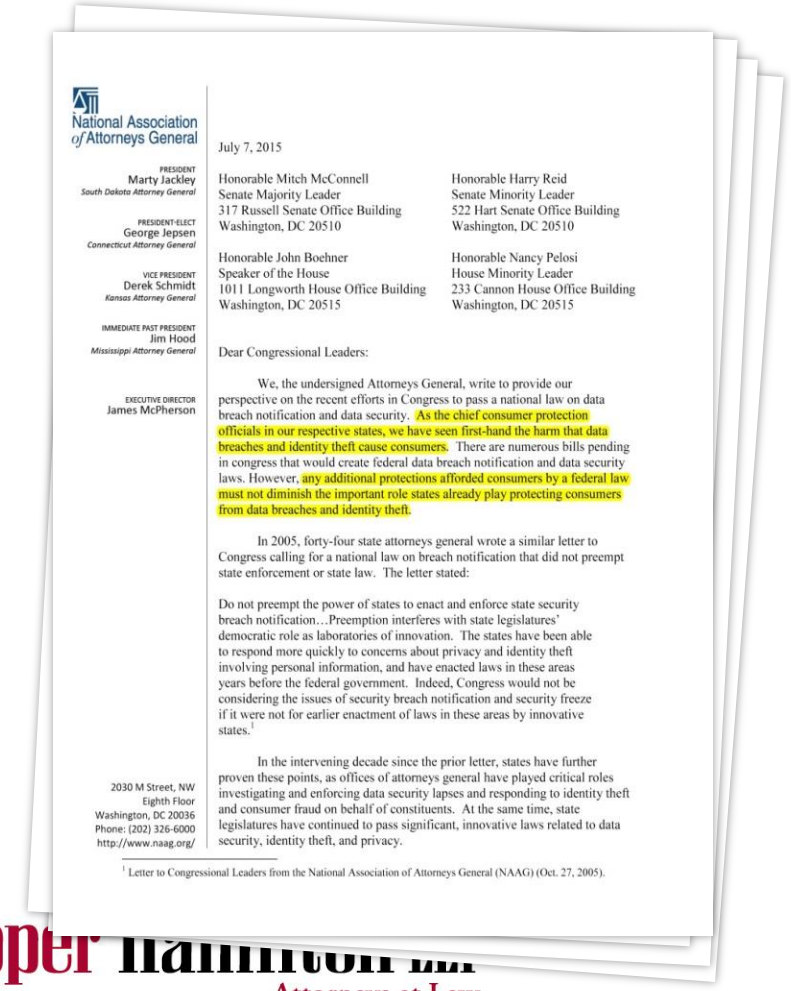
National Association of Attorneys General

- State Attorneys General Regulation and Enforcement

Pepper Hamilton LLP
Attorneys at Law

State AGs: Intense Interest

Letter to Congressional Leaders from the National Association of Attorneys General (Oct. 27, 2015)



National Association of Attorneys General

PRESIDENT
Marty Jackley
South Dakota Attorney General

PRESIDENT-ELECT
George Jepsen
Connecticut Attorney General

VICE PRESIDENT
Derek Schmidt
Kansas Attorney General

IMMEDIATE PAST PRESIDENT
Jim Hood
Mississippi Attorney General

EXECUTIVE DIRECTOR
James McPherson

July 7, 2015

Honorable Mitch McConnell
Senate Majority Leader
317 Russell Senate Office Building
Washington, DC 20510

Honorable Harry Reid
Senate Minority Leader
522 Hart Senate Office Building
Washington, DC 20510

Honorable John Boehner
Speaker of the House
1011 Longworth House Office Building
Washington, DC 20515

Honorable Nancy Pelosi
House Minority Leader
233 Cannon House Office Building
Washington, DC 20515

Dear Congressional Leaders:

We, the undersigned Attorneys General, write to provide our perspective on the recent efforts in Congress to pass a national law on data breach notification and data security. As the chief consumer protection officials in our respective states, we have seen first-hand the harm that data breaches and identity theft cause consumers. There are numerous bills pending in congress that would create federal data breach notification and data security laws. However, any additional protections afforded consumers by a federal law must not diminish the important role states already play protecting consumers from data breaches and identity theft.

In 2005, forty-four state attorneys general wrote a similar letter to Congress calling for a national law on breach notification that did not preempt state enforcement or state law. The letter stated:

Do not preempt the power of states to enact and enforce state security breach notification…Preemption interferes with state legislatures' democratic role as laboratories of innovation. The states have been able to respond more quickly to concerns about privacy and identity theft involving personal information, and have enacted laws in these areas years before the federal government. Indeed, Congress would not be considering the issues of security breach notification and security freeze if it were not for earlier enactment of laws in these areas by innovative states.[1]

In the intervening decade since the prior letter, states have further proven these points, as offices of attorneys general have played critical roles investigating and enforcing data security lapses and responding to identity theft and consumer fraud on behalf of constituents. At the same time, state legislatures have continued to pass significant, innovative laws related to data security, identity theft, and privacy.

2030 M Street, NW
Eighth Floor
Washington, DC 20036
Phone: (202) 326-6000
http://www.naag.org/

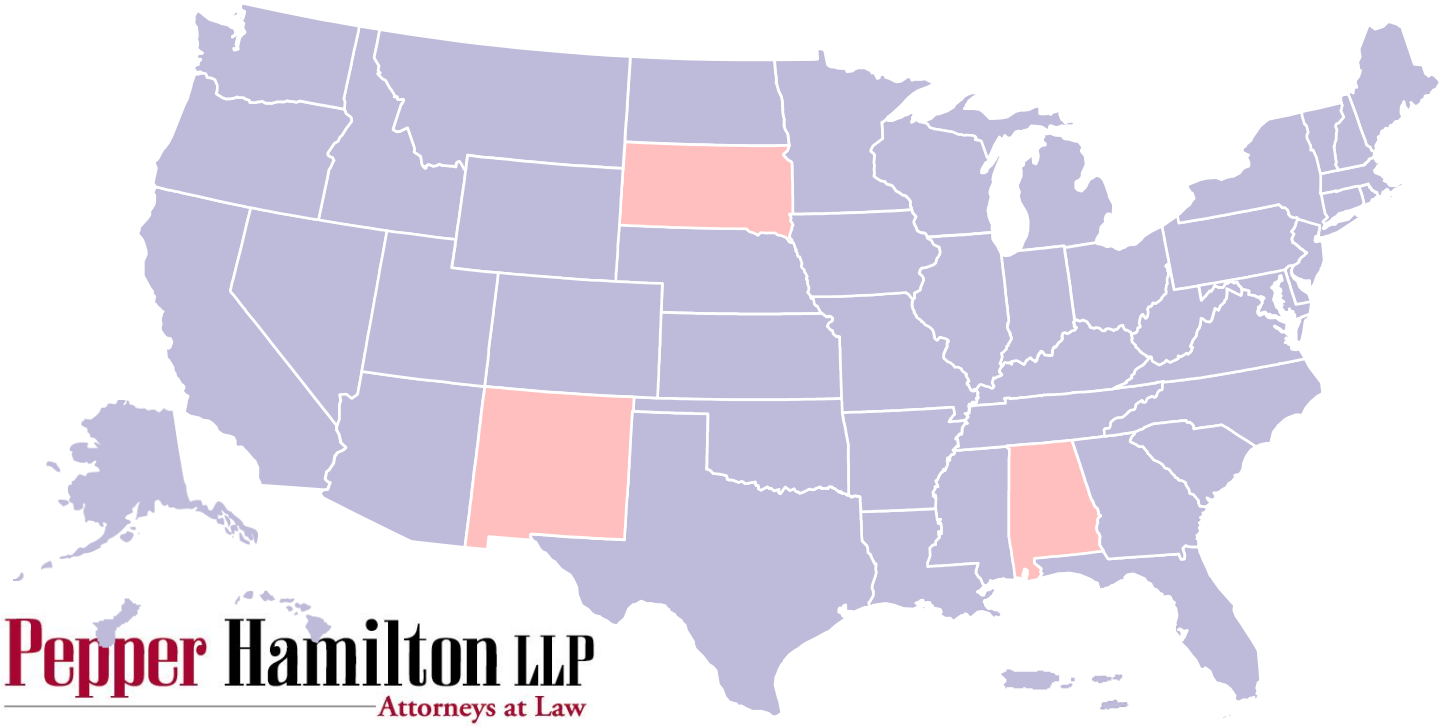
[1] Letter to Congressional Leaders from the National Association of Attorneys General (NAAG) (Oct. 27, 2005).

- Data Breaches and Identity Theft Cause Significant Harm to Consumers
- States Play an Important Role Responding to Data Breaches and Identify Theft
- Federal Law Should Not Preempt State Law
- Data Security Vulnerabilities Are Too Common

State AGs

Data Breach Notification Laws

- 47 states have enacted data breach notification laws
  - All require prompt notification of breach to consumers
  - Some require companies to adopt reasonable data security practices
- Provide for additional liability and impose civil penalties



Pepper Hamilton LLP
Attorneys at Law

State AGs

Enforcement Mechanisms

- What does a typical consent decree look like?
  - Penalties and fines dependent on the extent of the breach
  - Creation of new policies and procedures to ensure future compliance
  - Free identify theft protection/mitigation services
  - Mandatory audits and reporting back to State AGs
  - Creation of security based roles, including Chief Privacy Officer
  - Mandatory employee training on data security practices
  - Updates to technological infrastructure

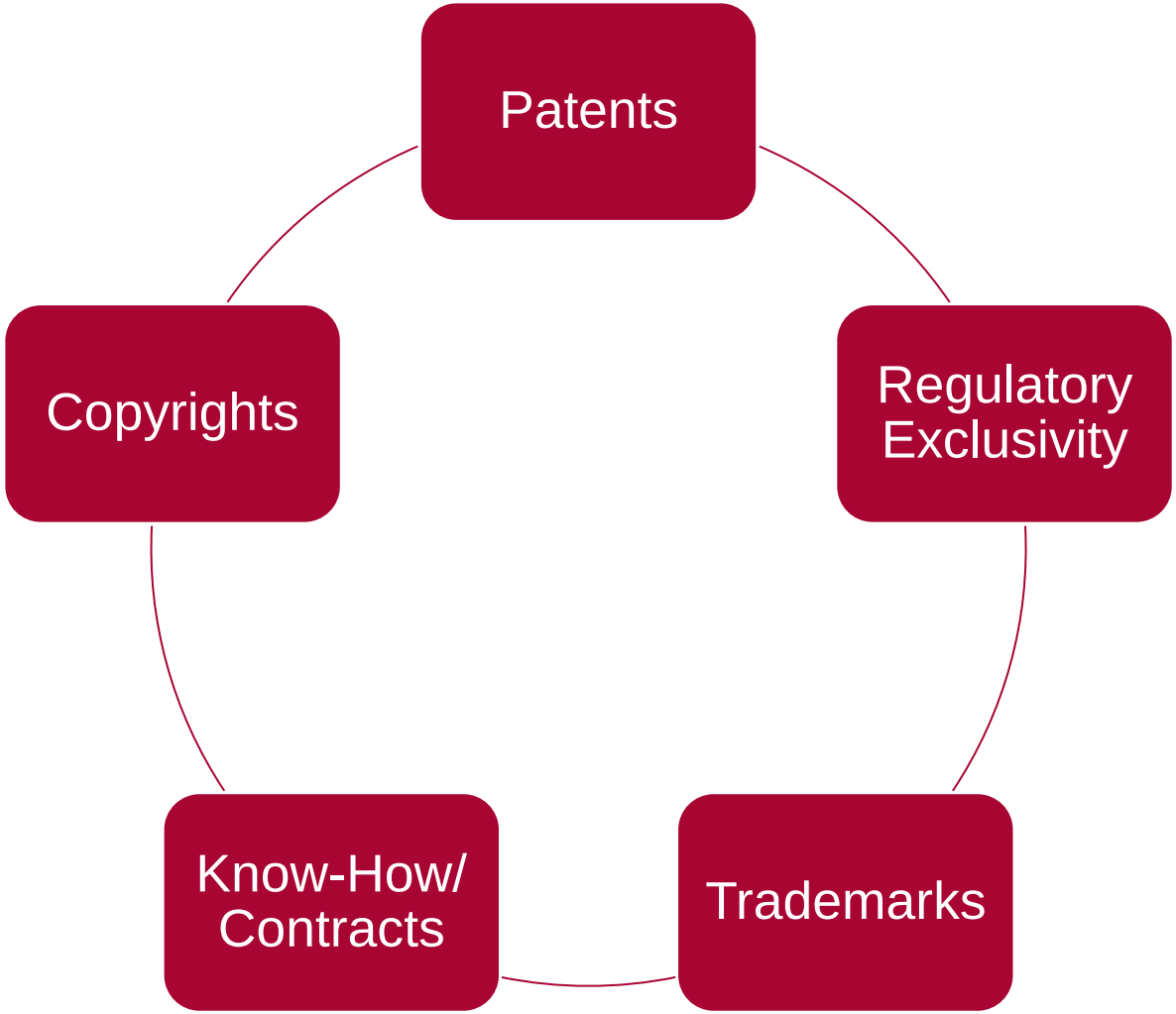
State AGs

Consumer Protection

- Violating Data Breach Disclosure Laws can be a violation of Unfair Trade Practices Act
- State consumer protection laws based on Section 5 of FTC:
  - "Capable of misleading"
  - "Violates public policy"
  - "Unfair"
  - "Concealing or omitting a material fact in selling product"
  - Misrepresenting "characteristics or benefits…"
- Injunctive relief, restitution, civil penalties, disgorgement
- No proof of harm to collect civil penalties

Patents only get you so far, for so long

- Increasing need to use different modes of protection



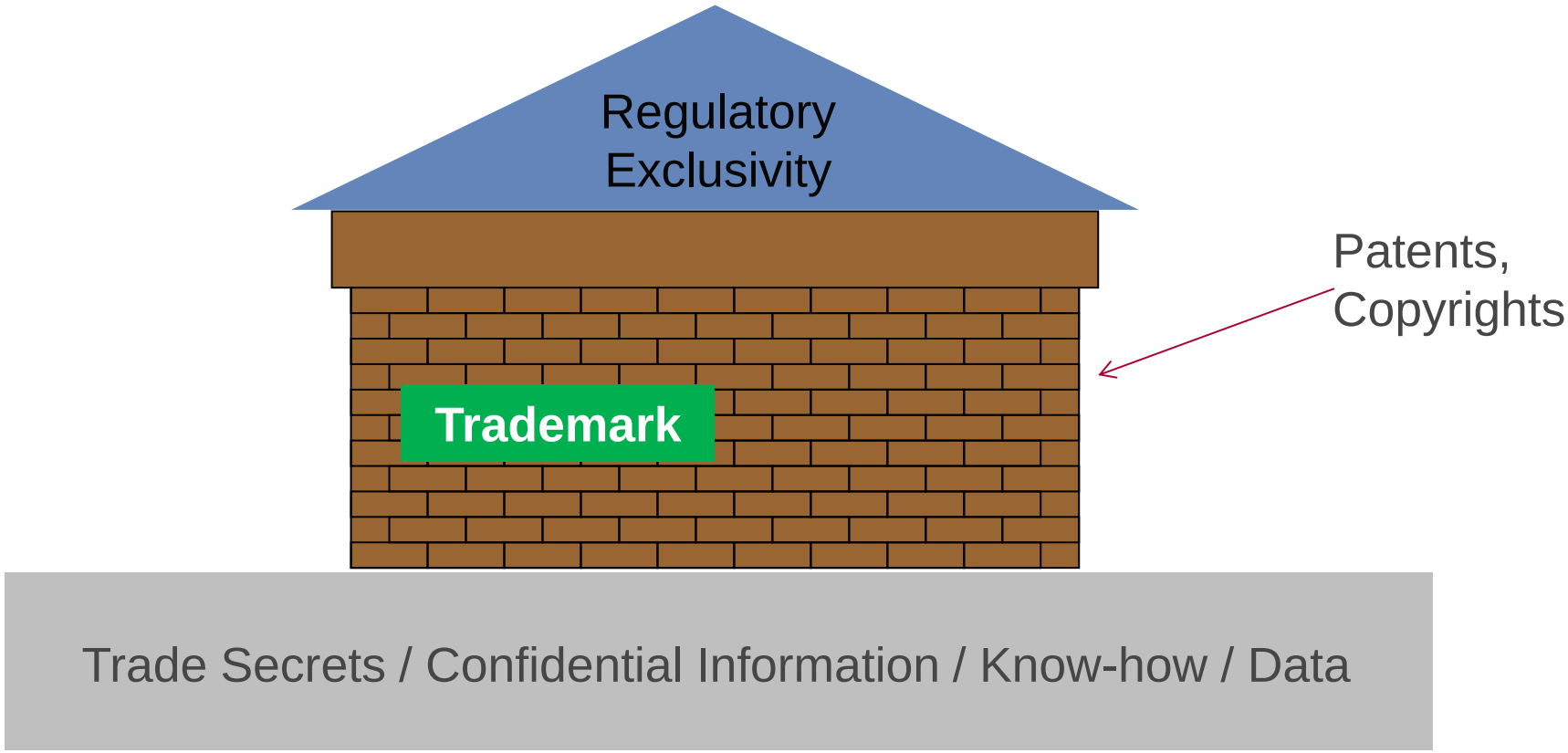
Pepper Hamilton LLP
Attorneys at Law

Protection Process

- Capturing IP internally
  - Think broadly, holistically
  - Anticipate future trends (e.g. use of big data / AI in clinical trial evaluation/reporting, responder analysis, reimbursement, post-market surveillance)
  - Educate and communicate with employees & advisors
- Collaborate externally
- Monitor competitors
- “Make Deal-Readiness a Daily Discipline” - Andrew Powell
  - Best practices for contracts and licensing, employees
  - Maintain organized IP database
  - IP due diligence mode / contemplate reps & warranties
  - Conduct regular internal audits

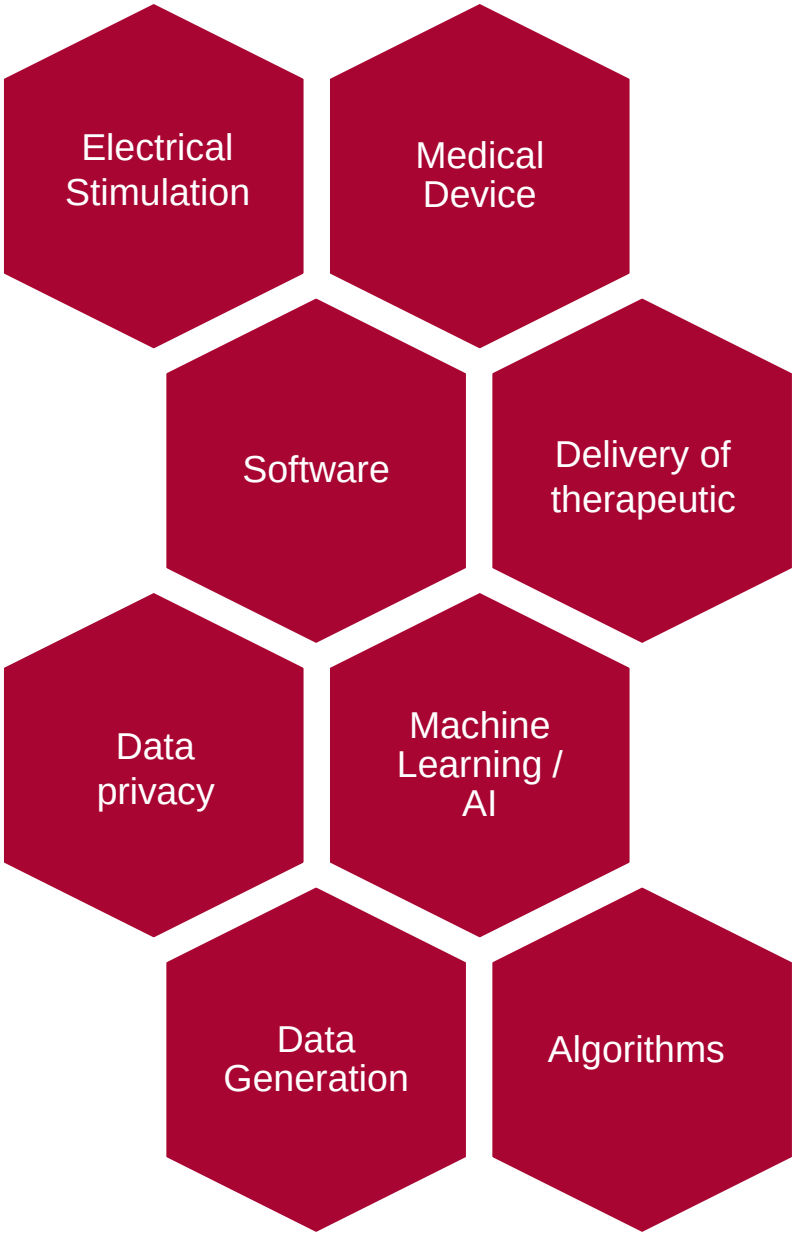
Integrated Fortress of IP

- Anticipate the need to educate on the value of “other” types of IP
- Build an integrated fortress *and present as such*



Pepper Hamilton LLP
Attorneys at Law

DBS – A Little Something for Everyone



Pepper Hamilton LLP
Attorneys at Law

Artificial Intelligence Applications for DBS

- Sensors gather neurological information and provide to Machine Learning/AI Algorithms (e.g., IBM's Watson)
  - Determine whether information matches identified patterns
  - Associate information with known patient issues for test data
  - Update and refine algorithms based on data
- Provide DBS / delivery of therapeutic / alert medical professional
  - Electrical and/or pharmacological stimulation to correct Parkinson's, dystonia, bipolar, OCD etc

How to Create and Protect IP for DBS

- We have worked with Dr. Rezai for 20 years
  - Coincidently, patent rights expire after 20 years
- Original subject matter developed by Dr. Rezai is entering the public domain just as DBS is advancing into new areas
- Newer developments are building upon the foundation of the original research
- Need to consider whether patent protection makes sense in light of design cycle

Pepper Hamilton LLP
Attorneys at Law

Patent Considerations

- Device
  - electrical and/or mechanical workings of the sensory, data storage and delivery and therapeutic storage and delivery components
- Method of using / implanting the device
  - surgical exception
- Method of making device
- Software…

Patent Considerations for DBS Software

- *Alice Corp.* – eligible subject matter
  - Software that is described and claimed functionally (based on what it does) is having significant issues at the PTO
  - Software should be claimed in terms of:
    - The system that is being improved OR
    - Structurally in terms of the software elements used to perform the operation
  - Software in a DBS system can be claimed as part of the system as a whole
  - Software can also be claimed based on the structural elements of the data flow (nodes in a neural network, linked lists, etc.)
  - Machine Learning algorithms have an inherent advantage of improving the machine on which they run

What Complementary Protections Exist?

- Trade Secret
  - What is a trade secret? Limitations?
  - Data Sets, algorithms- results in quicker approval, better patient outcomes
- Copyright
  - What does a copyright protect? Limitations?
  - Software
- Trademark
  - Brand recognized for accuracy, reliability, predictability, privacy / protection, patient-focused (DTC advertising)
  - Better reimbursement
- Data/Marketing Exclusivities
- Best practices for contracts / licensing

For more information, visit

www.pepperlaw.com

N. Nicole Stakleff
412-454-5869
staklefn@pepperlaw.com

Raymond A. Miller
412-454-5813
millerra@pepperlaw.com

Pepper Hamilton LLP
Attorneys at Law