Wireless Health Regulatory Issues

A 2015 Roadmap to FDA, FCC, and Privacy and Cyber Security Issues

February 26, 2015
Attorney Advertising

This presentation has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice or to invite an attorney-client relationship. Please consult your attorneys in connection with any fact-specific situation under federal, state, and/or local laws that may impose specific obligations on you and your company.

Cisco WebEx can be used to record webinars/briefings. By participating in this webinar/briefing, you agree that your communications may be monitored or recorded at any time during the webinar/briefing.

Attorney Advertising
Presented by

Robert Jarrin
Senior Director, Government Affairs, Qualcomm
rjarrin@qualcomm.com
(202) 263-0011
1. FDA Regulations Specific to Mobile Health Information Technologies

2. Developing an FCC Regulatory Checklist For mHealth Innovators and Investors

3. Cyber Security Considerations For The Wireless Health Sphere

4. Beyond HIPAA: The Evolving Landscape for Privacy Regulation
US FDA Regulatory Environment

Kim Tyrrell-Knott
Epstein Becker Green
Topics

- FDA regulation of Software
  - What is regulated, unregulated and subject to enforcement discretion
  - New guidance
    - MDDS
    - Wellness
    - Accessory
- Clinical Decision Support
- What’s Next?
FDA Regulation of Software
Changing Landscape – Dynamic and Deregulatory
Risk-Based Approach

- Mobile Medical App Guidance
- FDASIA Report
- MDDS Guidance
- 510(K) Exempt Devices Draft Guidance
- Wellness Draft
- Accessory Draft
- Clinical Decision Support*
### What Gets Regulated?

<table>
<thead>
<tr>
<th>Unregulated</th>
<th>Enforcement Discretion</th>
<th>Regulated</th>
</tr>
</thead>
<tbody>
<tr>
<td>• General purpose IT</td>
<td>• Electronic Health Records</td>
<td>• Meets definition of Medical Device</td>
</tr>
<tr>
<td>• Educational tools, medical textbooks</td>
<td>• Patient Portals</td>
<td>• Accessories to a medical device</td>
</tr>
<tr>
<td>• Facilitate patient access to information</td>
<td>• Trending, tracking and sharing data with healthcare providers</td>
<td>• Analyze patient-specific medical device data</td>
</tr>
<tr>
<td>• Administrative products</td>
<td>• Coaching app – support change in daily environment</td>
<td>• Transform platform into a medical device</td>
</tr>
<tr>
<td>• Health Management Health IT (Draft FDASIA Report)</td>
<td>• Medication Reminders</td>
<td></td>
</tr>
<tr>
<td>• Health and Wellness*</td>
<td>• Certain Telemedicine products</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Low Risk CDS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Medical Device Data Systems</td>
<td></td>
</tr>
</tbody>
</table>
Enforcement Discretion Examples
Medical Device Data System (MDDS)

Storage  Conversion  Medical Device Data
Transfer  Display

Active Patient Monitoring  Control Connected Medical Device
Modify  Analyze

Not active patient monitoring or controlling a device
Wellness Draft Guidance*

- Unregulated or Enforcement Discretion Wellness Products
  - Intended only for general wellness use
  - Low patient safety risk

- General Wellness Defined
  - Relates to maintaining or encouraging health/healthy activity
  - Associates healthy lifestyle with helping reduce risk or impact of chronic disease or condition where well established scientifically

- Applies only to CDRH

- Inclusion in guidance does not mean it is safe and effective; still subject to Consumer Product Safety Commission

*Draft guidance released 1/16/2015
Wellness Decision Tree

- Only General Wellness claims?
  - Yes
  - Claims relating to disease or condition?
    - Yes
    - Healthy lifestyle impact well understood?
      - Yes
      - “May help reduce risk or help living well” product claims?
        - Yes
        - Inherent risk to patient safety?
          - Yes
          - Not General Wellness Product
        - No
          - General Wellness Product
      - No
    - No
      - Not General Wellness Product
  - No
    - Not General Wellness Product

- No
  - Not General Wellness Product
## Wellness Claims Examples

<table>
<thead>
<tr>
<th>General Wellness Claims</th>
<th>Regulated Claims</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Claims to promote or maintain a healthy weight, encourage healthy eating, or assist with weight loss goals;</td>
<td>• A claim that a product will treat or diagnose obesity;</td>
</tr>
<tr>
<td>• Claims to promote relaxation, boost self esteem or manage stress - no reference to anxiety disorders or disease or condition;</td>
<td>• A claim that a product will treat an eating disorder, such as anorexia;</td>
</tr>
<tr>
<td>• Claims to improve mental acuity, instruction following, concentration, problem-solving, multitasking, management, decision-making, logic, pattern recognition or eye-hand coordination;</td>
<td>• A claim that a product helps treat anxiety;</td>
</tr>
<tr>
<td>• Claims to promote physical fitness, help log, track, or trend exercise, measure aerobic fitness, improve physical fitness, develop or improve endurance, strength or coordination, or improve energy;</td>
<td>• A claim that a computer game will diagnose or treat autism;</td>
</tr>
<tr>
<td>• Claims to promote sleep management, such as to track sleep trends;</td>
<td>• A claim that a product will treat muscle atrophy or erectile dysfunction;</td>
</tr>
<tr>
<td></td>
<td>• A claim to restore a structure or function impaired due to a disease, e.g., a claim that a prosthetic device enables amputees to play basketball.</td>
</tr>
</tbody>
</table>
Medical Device Accessory Draft Guidance*

- Accessory – a device that is intended to support, supplement and/or augment the performance of one or more parent devices
  - Not an accessory merely because it may be used with another device
  - Supplements if it adds new function or new way of using parent device
  - Augments if enables parent device to achieve intended use more safely and effectively; improves usability or convenience
  - Does not need to be necessary for parent device’s intended use

- Regulated Based on Risk
  - Look at accessory risk profile
  - Consider impact on parent device
  - Consider accessory risk independent of parent device

- Reclassification and De Novo

*Draft guidance released 1/16/2015
Dexcom Share Direct Secondary Display

- Secondary display
- Notify another person of CGM data in real time
- Receive/display
  - Real-time glucose values
  - Glucose trend data
  - Notifications and alarms
- Class II, 510(k) exempt
- Special controls

- Not intended for
  - making treatment or dosing decisions;
  - calculating insulin
  - modifying or analyzing data
  - receiving data directly from CGM
  - controlling device
  - replacing self monitoring or primary display
What Do We Know About CDS?
Clinical Decision Support

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
CDS - Enforcement Discretion Examples

- **Low Risk CDS**

- **Access to contextually relevant information**
  - Access to best practice treatment guidelines for common illnesses or conditions such as influenza based on patient diagnosis;
  - Drug-drug interaction or drug-allergy look-up tools.

- **Simple calculations routinely used in clinical practice**
  - BMI, APGAR Score NIH Stroke Scale, Mean Arterial Pressure

- **Checklist of common signs and symptoms to provide a list of possible medical conditions and advice on when to consult a health care provider**
Other CDS: Draft FDASIA Report

Evidence-based clinician order sets tailored for a particular condition, disease, or clinician preference;
Most drug dosing calculations; Drug formulary guidelines;
Reminders for preventative care;
Calculation of prediction rules and severity of illness assessments (e.g., APACHE score, AHRQ Pneumonia Severity Index, Charlson Index);
Duplicate testing alerts;
Suggestions for possible diagnoses based on patient-specific information retrieved from a patient’s EHR.

Not FDA Regulated

High risk clinical decision support
Computer aided detection/diagnostic software;
Remote display or notification of real-time alarms (physiological, technical, advisory) from bedside monitors;
Radiation treatment planning;
Robotic surgical planning and control;
Electrocardiography analytical software.

FDA Regulated
Clinical Decision Support is Regulated Today

Traditional Factors Considered

- Competent Human Intervention
- Transparency
- Time to reflect
- New Capabilities or Intended Uses
- Individualized Patient Care Recommendations
- Display, create, sound alarm or detect alarm conditions

How the Software Contributes to the User's Decision-Making

- Real Time, Active, or Online Patient Monitoring Functions
- Output is Provided or Manipulated in a novel or Non-Traditional Manner

CLINICAL DECISION SUPPORT
What Is Low Risk CDS?

IMDRF Report Focuses on

- Significance of information provided by SaMD to healthcare decision
  - Treat or Diagnose
  - Drive Clinical Management
  - Inform Clinical Management

- Seriousness of the Disease
  - Critical
  - Serious
  - Non-Serious

- **IMDRF is International Medical Device Regulators Forum – NOT FDA policy**
What’s Next?
Developing an FCC Regulatory Checklist
For mHealth Innovators and Investors

Paul Margie
Harris, Wiltshire & Grannis LLP
Overview

Who should understand FCC regulation of mHealth devices?

- Innovators building new technologies or services
- Investors performing a diligence on an mHealth company
- Transacting parties buying or selling a company with mHealth products

Why should you care about FCC regulations?

- Impact on product decisions on frequency, power, reliability
- Delay or interference closing on a transaction
- Violations can lead to fines, importation bans, or design changes
Overview

To establishing your FCC regulatory checklist, consider at least the following:

- **Frequency/Choice of Bands:**
  - What band will your product use and what rules apply to that band?
  - What interference must you avoid and accept?
  - Do you need a license and how do you transfer the license in a transaction?
  - What eligibility, power, and service rules apply?

- **Equipment authorization:**
  - Does your product need FCC equipment authorization?
  - How do you show compliance with technical rules (e.g.: SAR, power, directionality, OOBE)?

- **Labeling/disclosures:**
  - What logos, disclosures, and “magic words” must appear on or in your product, packaging, and user manual?

- **Accessibility rules:**
  - Do FCC accessibility rules apply?
  - Do you provide VoIP, “electronic messaging,” or “interoperable video conferencing”?
Frequency/Choice of Bands

The FCC has created a group of special bands for health-related devices, each with its own rules, and interference implications:

- **Medical Device Radiocommunications Service (MedRadio)**
  - Implanted and body-worn devices
  - 401-406 MHz for implantable; 401-402 and 405-406 MHz for body worn

- **Medical Micropower Networks (NMMs)**
  - Low-power network for functional electric stimulation
  - 413-419 MHz, 426-432 MHz, 438-444 MHz, 451-457 MHz

- **Medical Body Area Networks (MBANs)**
  - Wireless networking of body transmitters
  - 2360-2400 MHz

- **Wireless Medical Telemetry Service (WMTS)**
  - Transmission of medical telemetry to a monitoring location
  - 608-614 MHz, 1395-1400 MHz, and 1427-1432 MHz
Frequency/Band Choice

A closer look at the MedRadio Rules as an example:

- **Licensing/eligibility**: licensed by rule (no exclusivity/no auction), but limited to implanted and body-worn devices

- **Frequencies**: 401-406 MHz for implantable; 401-402 and 405-406 for body worn

- **Interference**: operated on a secondary, non-interference basis with primary government users – must design equipment to withstand interference from higher-power government users

- **Power**: maximum EIRP of 25 microwatts (note emission mask as well)

- **Emission bandwidth**: 100 kilohertz in 401-401.85 and 405-6 MHz; 150 kilohertz in 401.85-402 MHz; 300 kilohertz in 402-405 MHz;

- **Sharing**: mandated listen before talk -- except for devices using tighter power and duty-cycle rules, and required transmitter cooperation for sharing
Frequency

But mHealth devices can also use more generic FCC bands, each of which has its own rules and interference implications – for example:

- 2.4 GHz unlicensed band
- 5 GHz unlicensed bands
- Commercial mobile radio service (CMRS) licensed bands (with a carrier)
- Upcoming 3.5 GHz hybrid licensed/unlicensed band
Equipment Authorization

Options: “Verification” (no filing required), “Declaration of Conformity” (no filing required), or “Certification” (filing required)

- The FCC typically doesn’t review equipment itself – it has designated Telecommunications Certification Bodies (TCBs) to do this on its behalf

- Devices requiring certification often need lab testing to show compliance with RF safety (SAR) and rules and emissions limits, which can be time consuming and expensive

- TCBs will not certify devices presenting novel issues – here companies must work with the FCC through the Knowledge Database (KDB) process

- Successful certification yields an FCC ID – plan ahead, it can take months

- Companies may not import, market, or operate equipment prior to equipment authorization unless it is subject to one of the FCC’s limited exceptions (e.g. rules for experiments, tests, or trade shows)
Labeling and Disclosure

All intentional and unintentional radiators must comply with FCC labeling and user manual disclosure rules:

- Specific labeling requirements determined by the type of equipment and the equipment authorization procedure – for example for Part 15 devices:
  - Verification: “Unique identifier” and applicable disclosure statement
  - Declaration of conformity: FCC logo, trade name, and model number
  - Certification: FCC ID and applicable compliance statements
  - FCC allows some flexibility for small devices and recently permitted e-labeling for devices that have the capability to electronically display the label
  - Remember the EU rules as well (and note that compliance with the US and EU rules can potentially satisfy requirements in certain other countries)

- The FCC also requires that radiators include disclosures and “magic words” in user manuals, with the specifics determined by the type of device.

- Non-compliance can lead to the FCC blocking authorization, Customs denying import, and fines
Accessibility Rules

Is your product or service subject to FCC accessibility rules?

- The Communications and Video Accessibility Act expanded FCC jurisdiction and led to new accessibility rules for parties that may not see themselves as telecommunications providers

- Covered services: (1) interconnected VoIP, (2) non-interconnected VoIP, (3) “electronic messaging,” and (4) “interoperable videoconferencing”

- Obligations: must ensure products and services as accessible to and usable by individuals with disabilities unless doing so is not achievable, and must be compatible with accessible equipment if it is not achievable
  - Input, control, and mechanical features
  - Assessment of FCC “performance objectives”
  - Covered entities must maintain records demonstrating compliance
  - Enforcement: requests for dispute assistance, informal complaints, formal complaints – backstopped with fines and mandated compliance
Cyber Security Considerations For The Wireless Health Sphere

Adam C. Solander
Epstein Becker Green
Overview

MHealth

Security Rule

Privacy Rule

State Law

MHealth
Overview

HIPAA Privacy Rule:
The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other protected health information. The Rule requires appropriate safeguards to protect the privacy of protected health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

HIPAA Security Rule:
The HIPAA Security Rule establishes national standards to protect individuals’ electronic protected health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

State Law:
Forty-seven states, have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information. Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc); definitions of “personal information” (e.g., name combined with SSN, drivers license or state ID, account numbers, medical information etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).
Applicability

- **Practice Tip:** If you sign a BAA the provisions of the Privacy and Security Rules are applicable to you
  - Days of “If Applicable” coming to end

By Law + By Contract = HIPAA Compliance
The New Reality: Health and Device Industries Under Attack

“The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.”

- FBI Flash Alert, Aug., 2014
The Security Rule: In the Breach Age

- The Security Rule compatible with good IT security practices.
  - Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI
  - Compliance, product development, legal, and IT all have a role

- The “HIPAA Security Rule compliant” misnomer
  - Required and addressable implementation specifications
    - Risk Assessment (required)
    - Encryption (addressable)
  - Very few articulated controls
    - Organization specific
Risk Assessment

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
  - Foundation of security rule compliance
  - Cyclical: assessment and mitigation a process
  - Physical, administrative, and technical
    - Scanning, code review, policy, on-site
  - NIST 800-66

- Practice Tips
  - Attorney-client privilege
  - Assessor selection
  - Scope
  - Timing
  - GAP Assessment is not a risk assessment
What to Look For: Business Partners

- The Privacy Rule requires BAAs be signed with any downstream BA.
- Business partners often the weakest link in IT security
  - Diligence to ensure adherence to BAA and other contractual obligations
    - Would you buy this company?
    - What controls are most important to you?
  - Off-shore partners
    - Development, support, call centers etc.
  - Indemnification and financial footing
What to Look For: Employees

- HIPAA requires that employees be trained on their privacy and security obligations with respect to PHI
  - Many of the most damaging breaches have resulted from social engineering or employees with their own processes or data repositories
    - Organizations must assess whether their current training protects organization
    - Identify employees with processes outside of workflow

- Practice Tips
  - Understand what company information is available to con artists (social media, org charts etc.)
  - Develop protocol for transmitting sensitive data or system credentials (e.g. IT will never ask for this information)
  - Train on identification of fraudulent communications
  - Interview employees to determine whether secondary processes have been created
    - Ex., transmission, storage, and device
What to Look For: Response Plan

- **It’s not if, it’s when:** in a breach situation, response time and response effectiveness are critical

- **Incident response plan:**
  - Multidisciplinary
    - Must respond effectively while protecting organization
    - Chain of command
    - Articulated responsibility
  - Prepared
    - Clear protocol for triggering response team
    - Arrange for vendors before an incident happens
    - Understand reporting obligations
The Business Case for Security Compliance

- Companies with security issues face unprecedented levels of federal and state enforcement
  - Likely subject to state law even if HIPAA inapplicable
- Private plaintiff class actions
  - Nominal damages provisions
  - HIPAA often used as a standard
- Contractual Damages
  - Cost of breach: Average of $201 per record affected
  - Total costs rise to hundreds of millions
- Minor incidents now have a big effects on shareholder value and reputation
  - Incident effect largely dependent upon response
Take Away

- HIPAA or Similar State Law
- Device/Health Industry Under Attack and Unprepared
- Compliance and IT No Longer Separate
Beyond HIPAA: The Evolving Landscape for Privacy Regulation

Adrienne Fowler
Harris, Wiltshire & Grannis LLP
Overlapping Domestic Regulation of Consumer Data Collection, Use, and Security

- FDA
- DHS/DOJ
- FTC/DOJ
- FCC
- State AG's
FTC Act

- FTC jurisdiction
  - Extremely broad
  - Common carrier exception
  - HIPAA-covered entities probably not exempt

- State Little FTC Acts

- Remedies
  - FTC consent decrees
  - Consumer redress
  - Statutory fines
  - State private rights of action
FTC: Unfair and Deceptive Acts & Personally Identifiable Information

- Fundamentally case-by-case inquiries, with a few big picture rules

- “Deceptive” practices
  - Affirmative misrepresentations
  - Implied misrepresentations, context, and prominence
  - Safe harbor non-compliance
  - Covers all company statements, not just the privacy policy

- “Unfair” practices
  - Retroactive changes to treatment of data already collected without consent
  - Failure to maintain reasonable and adequate data security
  - Use of data inconsistent with context
FTC: Unfair and Deceptive Acts & Personally Identifiable Information

- **mHealth examples:**
  - Data security includes control over device functionality
  - Subcontractor and affiliate use of data and data security
  - Using previously collected consumer data in starting a new service
  - Permission re-delegation
  - Acquiring company will be bound by target’s promises
FTC: Children’s Online Privacy Protection Act

- Special rules for online services directed to young children (under 13) and online services that knowingly collect personal information from young children
- “Online services” and “personal information” are extremely broad terms
- Allowing users to enter age information + allowing use by consumers under 13 = knowingly collecting personal information from children under 13
  - COPPA is more likely to apply to mHealth and HealthIT services than other online services because age is more commonly collected.
FTC: Children’s Online Privacy Protection Act

- Comprehensive COPPA policy requires:
  - Enhanced notice to parents about data collection and use
  - Verifiable parental consent before information is collected, except in limited circumstances
  - Granting parental access to and right to delete information
  - Timely data deletion
  - Adequate data security
- Safe harbor programs
- Civil penalties of up to $16,000 per violation
State Attorneys General

- Little FTC Acts
- More specific legislation on privacy
  - Social security number collection
  - Spyware
  - Privacy notice requirements
- Data Breach Notification for non-HIPAA-covered entities
  - Limited federal requirements (currently)
  - Almost all states have data breach security notification laws
FCC CPNI Rules: Traditional Limits On Consumer Data Privacy

- CPNI: Certain data related to a consumer’s use of a telecommunications service

- Covered entities must:
  - Provide certain notifications to consumers
  - Obtain consumer consent before using CPNI for certain marketing activities
  - Take steps to prevent unauthorized access
  - Comply with recordkeeping and reporting requirements

- May apply to mHealth apps and devices with built-in interconnected VoIP

- New net neutrality rules likely to change who is covered by CPNI rules
FCC: Expanding Its Privacy Reach In TerraComm and YourTel America

- “Proprietary information” is protected
- Data security failures as unjust and unreasonable practice
  - Entities exempt from FTC jurisdiction under the common carrier exception will likely face similar regulatory scrutiny from the FCC
Questions?

Kim Tyrrell-Knott
Member of the Firm, Epstein Becker Green
ktyrrekknott@ebglaw.com
858-764-2494

Adam C. Solander
Member of the Firm, Epstein Becker Green
asolander@ebglaw.com
202-861-1884

Paul Margie
Partner, Harris, Wiltshire & Grannis LLP
PMargie@hwglaw.com
(202) 730-1352

Adrienne E. Fowler
Associate, Harris, Wiltshire & Grannis LLP
afowler@hwglaw.com
(202) 730-1343
Admitted only in NY; supervised by Brita Strandberg, member of the D.C. Bar, pending D.C. admission.
About Our Firms

About Epstein Becker Green

Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in offices throughout the U.S. and supporting clients in the U.S. and abroad, the firm’s attorneys are committed to uncompromising client service and legal excellence.

About Harris, Wiltshire & Grannis

Harris, Wiltshire & Grannis LLP is a boutique law firm with one of the leading telecommunications and technology practices in the United States. The firm represents industry-leading clients in a wide range of areas, including spectrum policy, wireless equipment regulation, IP services, international trade and investment, accessibility regulation, and litigation and appeals related to these topics. HWG has a national reputation as a go-to firm when Internet companies, service providers, equipment manufacturers, or investors face complex regulatory challenges, are involved in appellate litigation arising from regulatory decisions, or seek strategic guidance for bet-the-company decisions. HWG is also a transactions firm of choice for both major and routine telecommunications transactions for wireline, wireless, broadcast, and international clients.
Epstein Becker Green Resources


Join our group on LinkedIn! Mobile Medical Apps- mHealth Community

http://cdscoalition.org  http://mhealthregulatorycoalition.org/
Thank You.

www.ebglaw.com
www.hwglaw.com