Digital, Mobile, and Virtual Medicine: Legal Challenges

Ryan Johnson and Catherine London

May 11, 2016

Fredrikson & BYRON, P.A.

Today's Presentation

- Introductions
- Overview
- Virtual Medicine: Telehealth and Telemedicine
- mHealth
- Q&A

Overview

- Consumer-driven demand for accessible, affordable, quality health care.
- Convenience Care
  - Digital Health
  - mHealth
- Many Common Legal Issues
- Evolving Regulatory Landscape

Legal and Regulatory Issues

- Licensure
- Scope of Practice/Prescriptive Authority
- Reimbursement
- Corporate Practice of Medicine
- Fraud and Abuse
- FDA and FTC
- Privacy and Security
- Cybersecurity

What is Digital Health?

- Includes mobile health (“mHealth”), health information technology (“HIT”), wearable devices, telehealth and telemedicine, and personalized medicine.
- Investment in digital health is increasing.
  - In 2015, digital health venture startups raised a record $4.5 billion, up from $4.1 billion in 2014.

What is Virtual Medicine?

- Telehealth
- Online Diagnosis, Treatment, and Prescriptions
- Legal and regulatory issues are constantly evolving.

Licensure

- Practitioners must meet licensing requirements in the state where the patient is located.
- Key issue in any telemedicine arrangement.
- State laws regarding telemedicine vary:
  - Some state licensing laws directly address telemedicine and explicitly define the practice of telemedicine.
  - Some states laws indirectly address telemedicine by defining the practice of medicine to include diagnosing or recommending treatment through electronic means.
  - Some states are silent.

Licensure

- Some states require full licensure of practitioners providing telehealth services to patients in state.
  - "Active" or in-state practice requirements
- Some states have special telemedicine licenses (e.g., MN, MT).
- State Licensure Exceptions:
  - Physician-to-physician consults
  - "Infrequent" or "occasional" consultations (e.g., fewer than 10 consults per year)
- Multi-state licensure creates challenges.

Interstate Compact

- Relatively new, voluntary expedited pathway to licensure for qualified physicians who wish to practice in multiple states
- Enacted in 12 states and introduced in another 14.
  - More info at http://licenseportability.org/

Scope of Practice

- Use of non-physician practitioners increasing.
  - In telemedicine context, this raises issues regarding scope of practice, supervision, and prescriptive authority.
- Other considerations:
  - Written collaborative agreement requirements
  - Protocols
- Nurse Licensure Compact

Physician Supervision

- Levels of Supervision:
  - General supervision: Procedure must be furnished under physician's direction and control, but physician's presence not required.
  - Direct supervision: Physician must be present in office suite and immediately available.
  - Personal supervision: Physician must be in attendance in room during procedure.

Physician Supervision

- Direct supervision/on-site requirements can significantly impact telemedicine arrangements.
- Is remote supervision acceptable?
  - Non-physician practitioner and patient in same location, but supervising physician off-site.
- Must review state requirements.
  - Physician/non-physician practitioner practice ratios.

Prescriptive Authority

- Issues surrounding prescribing medication electronically in connection with telehealth encounters.
- Permissibility of remote prescribing varies significantly across states.
  - State pharmacy statutes and regulations
  - Licensing board policy
  - Medicaid reimbursement policies

Online Visits
Scope of Practice/Prescriptive Authority

- MDs v. NPs v. RNs v. PAs
- Physician supervision rules
  - Written collaborative agreement
  - Protocols
  - On-site requirements
  - Ratios

Online Visits
Prescriptive Authority

- Face-to-face requirements
- Existing patient relationships
- Strategies
- Future—payors, etc. pushing to clarify these requirements and accommodate online consultations.

Reimbursement

- Employers and Individuals
- Private/Commercial Payors
- Government Payors
  - Medicare
  - Medicaid
  - Other

States and Private Payors

- Wide range of telemedicine reimbursement policies among state Medicaid and private payors.

Medicare Reimbursement

- Limited Medicare reimbursement for Part B services furnished by a physician delivered via telemedicine to an eligible beneficiary.

Medicare Reimbursement

- Medicare reimbursement is available only if certain requirements are met regarding:
  - Geographic location of originating site,
  - Type of services provided,
  - Type of institution delivering the services, and
  - Type of health provider.

Originating Sites

- Originating site must be:
  - Rural Health Professional Shortage Area (HPSA);
  - County that is not a Metropolitan Statistical Area (MSA); or
  - Approved demonstration project.
- No limitation on location of distant-site health professional delivering the service.

Eligible Originating Sites

- Offices of a physician or practitioner
- Hospitals
- Critical access hospitals
- Rural health clinics
- Federally qualified health centers
- Skilled nursing facilities
- Hospital-based dialysis centers
- Community mental health centers

Eligible Distant Site Practitioners

- Physicians;
- Nurse practitioners;
- Physician assistants;
- Nurse midwives;
- Clinical nurse specialists;
- Clinical psychologists,
- Clinical social workers; and
- Registered dietitians or nutrition professionals.

Eligible Medical Services

- Consultations, office visits, individual psychotherapy and pharmacologic management delivered via a telecommunications system.
- Interactive audio and video telecommunications system must be used that permits real-time communication between distant site practitioner and patient.
  - Asynchronous “store and forward” technology only permitted in demonstration programs in Alaska and Hawaii.

Eligible Medical Services

- Reimbursement to professional delivering service via telecommunication is same as current fee schedule amount.
  - Submit CPT code for professional services with GT modifier (“via interactive audio and video telecommunications system”).
- Originating site is eligible to receive a facility fee.

Coverage

- Services delivered via telecommunications may be covered as physician services.
  - "A service may be considered to be a physician's service where the physician either examines the patient in person or is able to visualize some aspect of the patient's condition without the interposition of a third person's judgment." Medicare Benefit Policy Manual, Ch. 15, § 30.
  - Direct visualization is possible by means of x-rays, electrocardiogram, tissue samples, etc.

Corporate Practice of Medicine ("CPM") Prohibition

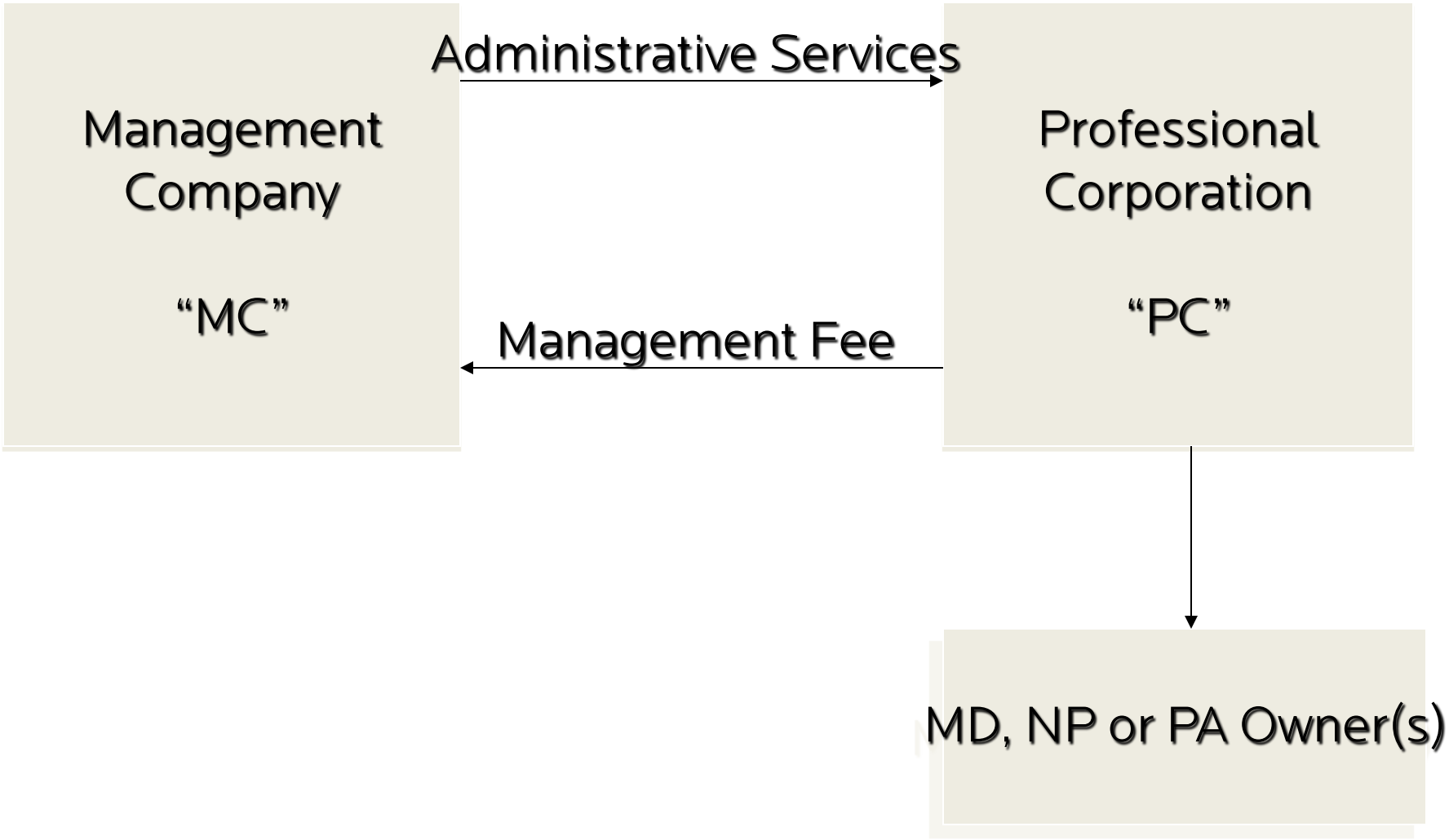
- CPM doctrine prohibits business corporations from employing medical professionals or owning medical practices.
  - Seeks to prevent lay control over medical judgment.
- CPM prohibition has been criticized by many scholars.

CPM Violations

- Potential Ramifications:
  - Refusal to pay claims
  - Injunction against continued operation of retail clinics
  - Criminal prosecution for engaging in the unauthorized practice of medicine
  - Entire arrangement could be declared void
  - Technical violation of certain fraud and abuse laws (e.g., the False Claims Act) by virtue of submitting claims to Medicare or Medicaid
  - Loss of “private practice”, “physician office” and similar exceptions from state licensing requirements (CON, lab license, etc.)

CPM (cont.)

- If state CPM prohibition applies to structure, the management company model may be an option.
  - Other options



CPM (cont.)

- Management agreement
  - long-term
  - restrictions on termination
  - restrictive covenant
  - management fee
  - management company can handle all non-clinical matters

CPM (cont.)

- Risks with management company structure:
  - Owners may seek to void the agreement.
  - May be viewed as a sham.

Fee-Splitting

- Most states prohibit fee-splitting.
  - Perceived danger of allowing professionals and non-professionals to share in income from professional services.
    - Temptation for the physician and nonprofessional to maximize profit through medically unnecessary services.
    - Temptation for the physician and the non-professional to limit medically necessary services in order to maximize income.

Federal Anti-Kickback Statute ("AKS")

- Prohibits the offering, paying, soliciting or receiving any remuneration in return for
  - business for which payment may be made under a federal health care program; or
  - inducing purchases, leases, orders or arranging for any good or service or item paid for by a federal health care program.
- Remuneration includes kickbacks, bribes and rebates, cash or in kind, direct or indirect.

AKS (cont.)

- Criminal and Civil Penalties
- Substantial monetary fines
- Imprisonment up to 5 years
- Civil Money Penalties
- False Claims Act exposure

AKS (cont.)

- Relationships that should be reviewed under the AKS (and similar state laws).
  - Relationship with supervising/collaborating physicians.
  - Relationship with others (management company, etc.).

AKS (cont.)

- No issue if federal health care programs are not involved.
  - But remember state anti-kickback prohibitions (for example, Minnesota Statutes, Section 62j.23).
- May be a reason to go “cash only”
  - Less risk but loss of income opportunity (e.g., Medicare and Medicaid).
- Safe harbor protection
- Advisory opinions

AKS Safe Harbors

- If an arrangement meets one of the applicable safe harbors, it is fully protected from both criminal and civil liabilities under the Anti-Kickback Statute.
  - However, failure to meet all of the requirements of a particular, applicable safe harbor does not make the conduct per se illegal.
- Conduct outside the safe harbors judged on a case-by-case basis.

Self-Referral Prohibitions
Stark

- The Stark law prohibits a physician from making a referral for certain designated health services ("DHS") to an entity with which the physician (or an immediate family member) has a financial relationship, unless one of its many exceptions applies.
- Stark also prohibits entities from submitting claims for DHS provided pursuant to a prohibited referral.

Stark (cont.)

- Stark is a strict liability statute, meaning that the intent of the parties is irrelevant for purposes of determining whether the law has been violated.
- Stark provides for monetary penalties per violation, plus requires the refund of amounts paid for illegally referred DHS.

Online Visits
Malpractice Risks

- Telemedicine/Online Consultations
  - What is the standard of care?
  - One example: *Hageseth v. The Superior Court of San Mateo County*, 59 Cal. Rptr.3d 385 (Cal. Ct. App. 2007).

Online Visits
Risk Management

- Risk Management
  - Peer review
    - robust physician supervision/chart review if NPs/PAs provide online consultations
  - Monitor developments in clinical practice guidelines
    - use evidence-based treatment guidelines
  - Check with insurance carrier
  - Limit scope of practice/services offered online
  - Address continuity of care

What is mHealth?

- mHealth refers to the use of mobile devices and wireless technologies in medical care.
- Estimated 500 million smartphone users worldwide used mobile health apps in 2015.
- Regulatory landscape is evolving.

Consumer-oriented medical apps proliferate

Number of apps found in the Apple and Google Play stores for various heart health conditions, as of April 2015

	APPLE APP STORE	GOOGLE PLAY
Exercise	6,312	120
Weight loss	3,881	250
Diabetes mellitus	1,175	180
Smoking	732	250
Cholesterol	265	120
Hypertension	214	250
Medication adherence	38	250

Source: American Heart Association

FDA and mHealth

- FDA regulates medical “devices,” as defined by the FD&C Act.
  - 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, or in the cure, mitigation, treatment, or prevention of disease, or
    - to affect the structure or function of the body.

FDA and mHealth

- FDA issued guidance on mobile medical apps in September 2013.
  - Explained FDA's oversight of mobile medical apps as devices and its focus on:
    - Apps that present a greater risk to patients if they don't work as intended, and
    - Apps that cause smartphones or other mobile platforms to impact the functionality or performance of traditional medical devices.

FDA and mHealth

- Updated (nonbinding) FDA guidance was issued February 9, 2015.
  - Identifies three categories of mobile medical apps:
    - 1) Apps FDA will not consider as medical devices even if they relate to health;
    - 2) Apps FDA will regulate as medical devices; and
    - 3) Apps for which FDA intends to exercise enforcement discretion.

FDA and mHealth

- FDA will focus on mobile apps that meet the definition of a “device” and:
  - are intended to be used as an accessory to a regulated medical device, or
  - transform a mobile platform into a regulated medical device.
- Focus is on functionality, not platform.
  - Intended use of mobile app is key.

FDA and mHealth

- Mobile apps that connect to a medical device to control the device or for use in patient monitoring or analyzing data.
  - FDA considers these to be an accessory to the device that extend the intended use and functionality of the device.
  - Example: App that controls delivery of insulin on insulin pump.

FDA and mHealth

- Mobile apps that transform a mobile platform into a medical device by using attachments, display screens, or sensors or by including functionalities similar to currently regulated devices.
  - Example: Attachment of blood glucose strip reader to mobile platform to function as a glucose meter.

FDA and mHealth

- Mobile apps that become a medical device by performing patient-specific analysis and providing patient-specific diagnosis, or treatment recommendation.
  - Example: Apps that use patient-specific parameters to calculate dosage or create a dosage plan for radiation therapy.

FDA and mHealth

- Examples of mobile apps that FDA will not regulate as medical devices:
  - Apps that provide electronic access to medical textbooks or reference materials.
  - Apps intended for general patient education or educational tools for medical training.
  - Apps that automate office operations in a health care setting and are not intended for use in diagnosis/cure of disease (e.g., billing programs).

FDA and mHealth

- Mobile apps for which FDA intends to exercise enforcement discretion.
  - Mobile apps that meet the regulatory definition of a “device” but pose minimal risk to patients and consumers.
  - FDA has authority to treat these as devices, but has chosen not to, because of their low risk (and the enormous task of taking on this flood of apps).

FDA and mHealth

- FDA will use discretion on apps that:
  - Help users with disease self-management without providing treatment suggestions (e.g., medication reminders);
  - Provide tools to track health (e.g., apps that log or track blood pressure);
  - Provide easy access to information related to health conditions or treatments (e.g., drug interaction apps);

FDA and mHealth

- FDA will use discretion on apps that (cont'd):
  - Help patients document or communicate potential medical conditions to providers (e.g., video conferencing portals);
  - Automate simple tasks for health care providers (e.g., BMI calculators); or
  - Enable patients or providers to interact with EHR systems.

FDA and mHealth

- FDA mobile medical apps policy does **not** apply to:
  - Entities that solely distribute mobile apps (e.g., “iTunes store”).
  - Licensed practitioners who create mobile medical apps solely for use in professional practice that are not generally available to be used by others.

FTC and mHealth

- FTC consumer protection laws prohibit unfair or deceptive trade practices.
  - Laws apply to all mobile apps.
- Disclosures must be clear and conspicuous.
- Endorsements are subject to truth in advertising requirements.

FTC and mHealth

- Advertising claims must have a "reasonable basis."
  - Health and safety claims must be supported by competent and reliable scientific evidence.
- FTC mobile medical app settlements:
  - UltimEyes Vision.
  - MelApp and Mole Detective.

FTC and mHealth

- FTC Best Practices:
  - Minimize data collected and retained and de-identify data, if possible.
  - Limit access to info and use permissions.
  - Keep authentication in mind and implement strong password protections.
  - Incorporate data security at every stage of the app's lifecycle: design, development, launch, and post-market.

FTC and mHealth

- FTC Best Practices (cont'd):
  - Perform due diligence and security testing to ensure third-party service providers and mobile platforms adequately protect data.
  - Use free and low-cost tools to safeguard consumers' personal information and help protect their privacy.
  - Communicate with users regarding app's security options and privacy features.

FTC and mHealth

- Mobile Health Apps Interactive Tool: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool
- Intended to help app developers understand what federal laws might apply to their apps.

Privacy and Security

- HIPAA's Applicability
  - Covered Entities
  - Business Associates
- Protected Health Information
  - Individually identifiable information (written, electronic, or oral) created or received by a provider;
  - Relating to an individual's health, provision of health care to an individual, or payment for health care;
  - That identifies the individual or provides a reasonable basis to identify the individual.

Privacy and Security

- HIPAA Privacy Rule
  - Prohibits uses or disclosures of PHI that are not permitted by the Privacy Rule.
  - Marketing is prohibited without patient's authorization.
  - "Marketing" is a "communication about a product or service that encourages recipients of the communication to purchase or use the product or service."

Privacy and Security

- Exceptions to marketing definition:
  - Communications for treatment of an individual by a health care provider or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual
    - unless the covered entity receives financial remuneration in exchange for making the communication.

Privacy and Security

- Exceptions to marketing definition (cont'd):
  - Communications to describe a health-related product or service provided by or included in a plan of benefits of the covered entity
    - unless the covered entity receives financial remuneration in exchange for making the communication.
  - Refill reminders for a currently prescribed drug or biologic.

Privacy and Security

- Other federal and state laws may impact the use of mHealth and wireless medical devices by consumers and health care professionals.
- Telephone Consumer Protection Act ("TCPA").
  - Enforced by the Federal Communications Commission ("FCC").
  - TCPA requires "prior express consent" from consumers before placing automated calls and texts to a consumer's wireless phone.

Privacy and Security

- TCPA consent requirements differ based on whether call/text contains a commercial or non-commercial message.
  - Call/text that contains a non-commercial message (e.g., appointment reminders) requires consent in writing, electronically, or verbally.
  - Call/text that contains a commercial message requires "express written consent."

Privacy and Security

- In a July 2015 Declaratory Ruling, FCC clarified application of TCPA to health care providers.
  - Providing a phone number to a provider constitutes “prior express consent” for health care calls subject to HIPAA by covered entities and business associates.
    - Exemption applies only to (i) calls or texts that are within the scope of the consent, and (ii) health care-related messages by a provider.

Privacy and Security

- Ruling also clarified limited exemption for health care-related calls and texts for which there is exigency and which are made for health care treatment purposes:
  - Appointment and exam confirmations and reminders; wellness checkups; hospital pre-registration instructions; pre-op instructions; lab results; post-discharge follow-up; Rx notifications; and home health instructions.
  - Additional requirements apply.

Privacy and Security

- HIPAA Security Rule requires implementation of administrative, physical, and technical safeguards to protect electronic PHI.
- Covered entities and business associates must:
  - Ensure the confidentiality, integrity and availability of ePHI that it creates, receives, maintains or transmits;
  - Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI;
  - Protect against impermissible uses or disclosures;
  - Ensure compliance by all workforce members.

Privacy and Security

- In deciding on security measures to use, covered entities and business associates must consider the following issues:
  - Organization size, complexity, and capabilities;
  - Organization's technical infrastructure, hardware, and software security capabilities;
  - Costs of security measures; and
  - Probability and criticality of potential risks to ePHI.

Cybersecurity

- Cybersecurity risks in health care are constantly evolving.
  - Must consider mobile devices, networked medical devices, EHRs, interoperable health IT systems, etc.
  - Sophisticated phishing and ransomware attacks can target entire HIT systems.
    - Ransomware attack on MedStar Health required provider to take its EHR offline for several days.

Cybersecurity

- Growing emphasis on medical device cybersecurity in recent years, given the proliferation of devices that connect to internet and provider networks.
  - August 2015 FDA safety warnings regarding Hospira's Symbiq medication infusion pump.
  - First time FDA warned providers to stop using a product due to cybersecurity risk.

Cybersecurity

- In October 2014, FDA issued guidance to assist companies submitting 510(k) and PMAs to ensure submissions adequately address cybersecurity.
- January 2016 draft guidance issued by FDA addresses post-market cybersecurity expectations.

Cybersecurity

- Post-market guidance recommends that manufacturers monitor, identify and respond to cybersecurity vulnerabilities as part of routine post-market surveillance.
  - Emphasizes importance of participation in an Information Sharing Analysis Organization.
- Issued shortly after 2016 OIG Work Plan.

Cybersecurity

- FDA recommends implementation of a cybersecurity risk management program as part of compliance with Quality Systems Regulation.
- Program components should include:
  - Monitoring cybersecurity info sources to identify and detect vulnerabilities and risk;
  - Understanding, assessing and detecting presence and impact of a vulnerability;

Cybersecurity

- Program components should include (cont'd):
  - Processes for vulnerability intake/handling;
  - Adopting a coordinated vulnerability disclosure policy and practice;
  - Deploying mitigations that address risk early;
  - Defining essential clinical performance to protect, respond and recover from cybersecurity risk; and
  - Applying 2014 NIST Framework for Improving Critical Infrastructure Cybersecurity.

Cybersecurity

- Takeaways:
  - Threat landscape is constantly evolving.
    - Digital health creates new vulnerabilities.
  - Risk assessments are as important as ever.
  - Know your vulnerabilities and be prepared for a breach.
  - Cyber liability insurance?
  - Be careful with legacy devices.

Questions?

Presenters

Ryan S. Johnson
Fredrikson & Byron, P.A.
612.492.7160
rjohnson@fredlaw.com

Catherine E. London
Fredrikson & Byron, P.A.
612.492.7464
clondon@fredlaw.com