Privacy and Data Security for Life Sciences and Health Care Companies

Mark A. Kadzielski, Sharon R. Klein, Dayna C. Nicholson | January 23, 2014

Pepper Hamilton LLP
Attorneys at Law

We will be starting momentarily…

Pepper Hamilton LLP
Attorneys at Law

Listen to the audio portion of today's webinar by dialing:

North America: +1.866.322.1348

International: +1.706.679.5933

Audio Conference ID: #43215867

Technical Support Numbers

If you experience technical difficulties, hit *0 on your telephone keypad and an operator will assist you.

Or you can dial:

For Web Support:
+1.877.812.4520 or
+1.706.645.8758

For Audio Support:
+1.800.374.2440 or
+1.706.645.6500

Feel free to submit text questions throughout the webinar

Privacy and Data Security for Life Sciences and Health Care Companies

Mark A. Kadzielski, Sharon R. Klein, Dayna C. Nicholson | January 23, 2014

Pepper Hamilton LLP
Attorneys at Law

Privacy and Data Security for Life Sciences and Health Care Companies

Click this icon to download the slides

Mark A. Kadzielski, Sharon R. Klein, Dayna C. Nicholson | January 23, 2014

Pepper Hamilton LLP
Attorneys at Law

Moderator: Mark A. Kadzielski

213.928.9820
kadzielskim@pepperlaw.com

- Partner and head of the Health Care Services practice of Pepper Hamilton LLP, resident in the Los Angeles office.
- Represents hospitals, medical staffs, managed care enterprises, and institutional and individual health care providers throughout the United States. His work includes government regulatory investigations, contracting issues, credentialing, peer review, licensing, medical staff bylaws, joint commission accreditation and Medicare certification.
- Has prepared more than 200 sets of medical staff bylaws and has handled numerous peer review hearings and appeals, including litigation in many courts.

Speaker: Sharon R. Klein

949.567.3506
kleins@pepperlaw.com

- Partner in the Corporate and Securities Practice Group
- Partner in charge of the firm's Orange County office and chair of the Privacy, Security and Data Protection practice
- Handles a variety of corporate and intellectual property matters, in particular, helping information technology and telemedicine clients grow and succeed
- Commissioner of the Electronic Healthcare Network Accreditation Commission (EHNAC), a voluntary, self-governing standards development organization established to develop standard criteria and accredit organizations that electronically exchange health care data.

Speaker: Dayna C. Nicholson

213.928.9807
nicholsond@pepperlaw.com

- Senior associate in the Corporate and Securities Practice Group of Pepper Hamilton LLP, resident in the Los Angeles and Orange County offices.
- Focuses her practice on health care-related matters, such as licensing and other regulatory compliance, peer review and credentialing, and corporate and medical staff governance. Her clients include hospitals, medical staffs, managed care organizations, medical groups, medical device retailers and other health care providers.
- Also has significant experience in patient information privacy issues, appeals of state-issued administrative penalties, Medicare and Medi-Cal certification, emergency care requirements, and litigation arising out of peer review matters.

TODAY'S TOPICS

- Mobile Health
- Regulatory Framework
- Practical Takeaways
- Questions

MOBILE HEALTH: A BRAVE NEW WORLD OF REGULATION

Pepper Hamilton LLP
Attorneys at Law

MOBILE HEALTH: A BRAVE NEW WORLD OF REGULATION

Proliferation of smart medical devices comes with vulnerabilities and a confusing web of regulations

- Cybersecurity incidents increasingly likely in wireless and network-connected devices transferring data electronically
- With increased risk comes increased regulation

EXPANSION OF REGULATORY PURVIEW

- Regulatory overlap
- Mobile health and medical devices are subject to multiple privacy/security regulations
  - FDA
  - FCC
  - FTC
  - ONC
  - HHS/OCR
  - State Law

CONSISTENCY ACROSS REGULATIONS

- National Institute of Standards and Technology (NIST)
- Privacy by Design
- Transparency
- Control
- Simplify Patient Choice
- Security

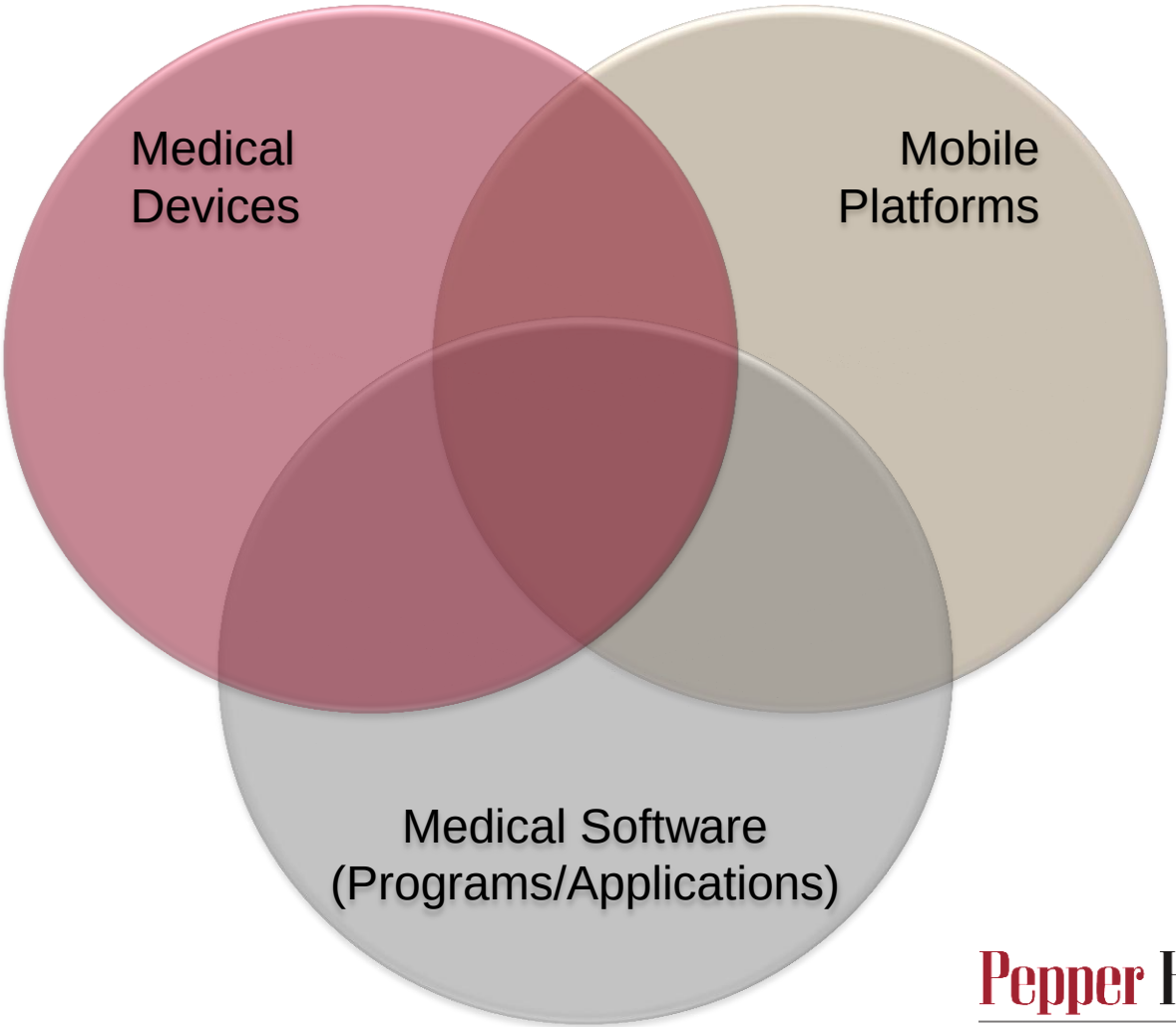
CHALLENGES ACROSS REGULATORY AGENCIES

- No pre-emption
- Inconsistent provisions
- Additional audits
- Cumulative fines/penalties

REGULATORY FRAMEWORK

REGULATORY FRAMEWORK

Food & Drug Administration



REGULATORY FRAMEWORK

Food & Drug Administration

- Mobile Medical Applications (Guidance, Sep 25, 2013)
  - Software as a Medical Device
  - FDA intends to regulate mobile medical software that poses a threat to public safety
  - Which software applications will be regulated?

REGULATORY FRAMEWORK

Food & Drug Administration

- Mobile Medical Applications
  - The key regulatory factor is the **intended use** of the mobile health application

REGULATORY FRAMEWORK

Food & Drug Administration

- Mobile Medical Applications
  - Regulated Applications:
    - Extending the medical device to control the device or to display device data
    - Using attachments, screens, sensors to transform a mobile platform into a medical device
    - Performing patient specific analysis
    - Assisting with diagnosis or treatment recommendations

REGULATORY FRAMEWORK

Food & Drug Administration

- Mobile Medical Applications
  - Non-Regulated Applications
    - Supplementing clinical care by helping patients manage their health
    - Providing patients with tools to organize/track health information
    - Providing easy access to patient's health conditions
    - Helping patients document or communicate medical information to providers
    - Performing simple calculations used in clinical practice
    - Enabling individuals to interact with PHRs and EHRs

REGULATORY FRAMEWORK

Food & Drug Administration

- Mobile Medical Applications
  - Regulatory Requirements
    - Establishment Registration and Medical Device Listing
    - Investigational Device Exemption (IDE) requirements
    - Labeling requirements
    - Premarket submission for approval or clearance
    - Quality System Regulation (QS Regulation)
    - Medical Device Reporting (MDR) (Adverse event reporting)
    - Correcting Problems

REGULATORY FRAMEWORK

Food & Drug Administration

- Medical Devices
  - Threats to medical devices
  - Ramifications of cybersecurity breaches

REGULATORY FRAMEWORK

Food & Drug Administration

- Management of Cybersecurity in Medical Devices
  (Draft Guidance, Jun 14, 2013)
  - Information Security Requirements
    - Confidentiality
    - Integrity
    - Availability
  - Security Guidelines
    - Limited Access
    - Trusted Content
    - Fail-Safe & Recovery Measures
  - Emergency Issues

REGULATORY FRAMEWORK

Food & Drug Administration

- Management of Cybersecurity in Medical Devices
  - Documentation
    - Risk Analysis
    - Update Control
    - Disabling Code
  - Industry Response
    - Existing devices
    - No retroactive implementation
    - Transition period
    - Intended Use
- Radio Frequency Wireless Technology in Medical Devices (Guidance, Aug 14, 2013)

REGULATORY FRAMEWORK

Federal Communications Commission

- Regulates the airwaves
- Wireless technology issues
- Wireless co-existence with electromagnetic compatibility
- Root cause analysis of problems with connectivity
- 802.11 wireless data security not robust

REGULATORY FRAMEWORK

Federal Trade Commission

FTC Chairman Edith Ramirez:

"Like a vigilant lifeguard, the FTC's job is not to spoil anyone's fun but to make sure that no one gets hurt."

REGULATORY FRAMEWORK

Federal Trade Commission

- Congress has been unable to pass a Federal Privacy Bill.
- Protecting Consumer Privacy in Era of Rapid Change (Report, Mar 2012)
  - Blue print for potential federal legislation, currently self-regulatory best practices.
  - "Privacy by Design":
    - Promote privacy throughout the organization and at every stage of development of products and services
    - Delete consumer data no longer needed and allow consumers to do the same
    - Provide reasonable security for data
    - Limit collection of data (consistent with context of particular transaction)
    - Implement reasonable data retention and disposal policies
    - Maintain reasonable accuracy of data

REGULATORY FRAMEWORK

Federal Trade Commission

- Protecting Consumer Privacy in Era of Rapid Change
  - Simplify Consumer Choice:
    - Provide consumer choice for any communications not related to original transaction
    - “Do Not Track” mechanisms allow consumer to control collection and use of their online data
    - Certain choices require consumer to “opt in”
  - Improve Transparency to Consumers:
    - Clearer and shorter privacy notices
    - Provide access to consumer data
    - Educate consumers about company’s data privacy practices

REGULATORY FRAMEWORK

Federal Trade Commission

- Mobile Privacy Disclosures, Building Trust Through Transparency (Report, Feb 2013)

REGULATORY FRAMEWORK

Office of the National Coordinator for Health IT

- HIT coordination
- Meaningful use
- Direct protocol under VA
- Secure email/fax
- Facilitates interoperability
- Promotes electronic medical records
- Not focused on patient safety

REGULATORY FRAMEWORK

HHS – Office of Civil Rights

- HIPAA/HITECH/Omnibus Final Rule
  - Business associates & Subcontractors
  - Direct Enforcement
  - Security Rule
    - Risk assessment
    - Technical, Physical, Administrative Safeguards
    - Policies & Procedures

REGULATORY FRAMEWORK

HHS – Office of Civil Rights

- HIPAA/HITECH/Omnibus Final Rule
  - Breach Reporting
  - Privacy Rule
    - Patient Access
    - Permitted disclosures for FDA regulated activities
    - Sale and marketing of information
    - Research

REGULATORY FRAMEWORK

Information Security & Privacy Board (ISPAB)

- Responsibility for cybersecurity in medical devices is too diffuse
- Recommendations (Mar 30, 2012)
  - Single government entity
  - FDA/NIST collaboration
  - Training and education
  - Defined reporting categories
  - Additional study

REGULATORY FRAMEWORK

State Law

- Privacy/Security of patient information
- Breach reporting
- Licensing
- Telemedicine/telehealth

PRACTICAL TAKEAWAYS

PRACTICAL TAKEAWAYS

- Appoint committee to monitor relevant regulatory guidances
- Educate developers of mobile medical applications when regulatory line(s) are crossed
- Keep software separate from regulated medical devices
- Follow and document privacy/security and quality principles
- Take precautions to eliminate malware contamination
- Monitor network connectivity for misuse

PRACTICAL TAKEAWAYS

- Perform and update risk analysis for security/privacy
- Develop incident response programs especially for life sustaining devices
- Obtain consent for collection of personally identifiable information
- Look for common compliance principles across regulatory agencies
- Document compliance with privacy/security criteria

Questions & Answers

Pepper Hamilton LLP
Attorneys at Law

Contact Brian Dolan at dolanb@pepperlaw.com for CLE Information

Pepper Hamilton LLP
Attorneys at Law

Thank You!

Mark A. Kadzielski
213.928.9820
kadzielskim@pepperlaw.com

Sharon R. Klein
949.567.3506
kleins@pepperlaw.com

Dayna C. Nicholson
213.928.9807
nicholsond@pepperlaw.com

Pepper Hamilton LLP
Attorneys at Law

For more information, visit www.pepperlaw.com

Pepper Hamilton LLP
Attorneys at Law