Privacy and Data Security: A Webinar for Life Sciences and Health Information Technology Companies

September 10, 2015

WILMERHALE

Attorney Advertising

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and New York*
- WebEx customer support: +1 888 447 1119, press 2

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Boards. Attendees requesting CLE credit must attend the entire program.*

Speakers

Jonathan G. Cedarbaum
Partner
WilmerHale

Barry J. Hurewitz
Partner
WilmerHale

Brian A. Johnson
Partner and Vice Chair, Corporate Practice Group
WilmerHale

Agenda

- Underlying principles of data privacy regulation
- Overview of health data regulatory standards
- Special health data regulatory considerations for life sciences and health IT companies

- Overview of cybersecurity preparedness
- Steps for cybersecurity incident response
- Two recent developments: (i) FDA and medical devices; (ii) NIST and EHRs on mobile devices

Categories of Data

- Non-personal, proprietary commercial and financial information
- Information pertaining to people
  - Human resources
  - Customers
  - Contractors, vendors, service providers
  - Third parties (e.g., patients, research subjects)
- “Personally identifiable information” is an important but declining differentiator
  - FTC has noted the “diminishing distinction” between PII and supposedly anonymous or de-identified information

Foundations of Information Governance

Regulatory Framework

- Fair Information Practices
- Generally applicable privacy laws
- Federal sector-specific privacy laws
- International data protection regimes

Cybersecurity

- NIST Cybersecurity Framework 1.0 (Feb. 2014)
- Enterprise risk management, not IT
- Humans, not just machines: governance, training, culture
- Incident response and preparedness

Fair Information Practices

- Widely accepted data privacy norms
- Evolved since 1973
- Reflected in most privacy laws & regulations

Fair Information Practice Principles
Notice / Awareness
Choice / Consent
Access
Integrity/ Security
Enforcement / Redress

State Data Regulation

- Invasion of privacy
- Notice requirements
  - Privacy policies on websites and in mobile apps
  - Disclosure of marketing uses of personal data
- Identity theft prevention
  - Risk-based Information Security Plans
- Online advertising
- Recorded communications
- Breach notification

Federal Sector-Based Data Regulation

FTC Section 5 “unfair” or “deceptive” practices	
Consumer/financial	Gramm-Leach-Bliley, FCRA
Government records	Privacy Act
Communications	ECPA, Cable Act
Children/students	COPPA, FERPA
Health/medical	HIPAA

Health & Medical Information Regulation

- Health Insurance Portability & Accountability Act of 1996 (HIPAA)
- Health Information Technology for Clinical & Economic Health (HITECH) Act of 2009

HIPAA / HITECH Regulations
Transactions, Code Sets and Identifiers
Privacy
Security
Breach Notification
Enforcement

HIPAA: Who's Covered

- **Applies to entities, not products**
  - But products can facilitate compliance by their users
- **Covered Entities**
  - Health plans
  - Health care providers that do standard electronic transactions
  - Health care clearinghouses that convert data among formats
- **Business Associates**
  - Not part of covered entity's workforce
  - Functions on behalf of the covered entity: Claims processing, data analysis, utilization review, quality assurance, billing, benefit management, practice management, repricing
  - Services to the covered entity: Legal, actuarial, accounting, consulting, data aggregation, management/administrative, accreditation, financial, data transmission, PHR vendors

HIPAA: What's Covered

- **Protected Health Information**
  - Individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for such health care
- **Statistical de-identification standard**
  - Person with "appropriate knowledge of and experience with" statistical and scientific de-identification principles and methods
  - Determines that the risk is "very small" that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual
  - Documentation of the analysis
  - This standard is inherently ambiguous
- **Safe harbor de-identification standard**

HIPAA: De-identification

- **Safe harbor de-identification standard**

Remove all of the following fields:

Names	Address (to 3 digit ZIP)	**Dates** & ages >90
Telephone	Facsimile	Email
Social security	Medical record	Health plan ID
Account number	Certificate/license	Vehicle ID
Device ID	URL	IP address
Biometric ID	Facial photo	Other unique code

- Proviso: No actual knowledge that the remaining information can be used to identify an individual

HIPAA: Privacy Rule

- "Minimum necessary" rule
- Permitted use and disclosure for treatment, payment and health care operations
- Notice of privacy practices issued by covered entities
- Choice
  - Uses and disclosures with authorization (opt in)
  - Uses and disclosures with opportunity to object (opt out)
  - Uses and disclosures with no choice
- Right to access and amend records
- Right to accounting of disclosures of one's data

Health Data Privacy

- State health data privacy laws and regulations address a wide range of issues beyond HIPAA
  - State *genetic privacy* laws vary
  - HIPAA defines a “floor,” not a “ceiling”
  - For example, California health data laws address:
    - Confidentiality of medical information, including by contractors
    - Consent for collecting health data for marketing
    - Patient rights to access records maintained by providers
    - Nondisclosure of HIV status, STD and hepatitis tests, prenatal tests and substance abuse information
    - Minors’ consent to treatment

HIPAA Security Standards

- Standards for protecting the confidentiality, integrity, and availability of electronic PHI

Physical	Technical	Administrative
Facilities	Access control	Oversight
Workstations	Integrity	Policies & procedures
Devices & media	Authentication	Awareness & training
	Transmission	Incident response
	Audit	Evaluation
	Encryption	Subcontractors

HIPAA: Breach Notification

- "Breach"
  - Unsecured PHI
  - Acquired, accessed, used, or disclosed in a manner not otherwise authorized
  - Subject to assessment of whether the information has been "compromised"
- "Unsecured PHI"
  - PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified in **HHS guidance**
- Notification by CEs
  - To individuals, HHS, and (if affecting 500+ persons) media

HHS Guidance on Securing PHI

PHI is deemed to be “secured” if:

- Encrypted in accordance with
  - Data at rest: NIST Special Publication 800-111
  - Data in motion: NIST Special Publications 800-52, 800-77 or 800-113 or others which are Federal Information Processing Standards (FIPS) 140-2 validated

  -- OR --

- Media on which the PHI is stored or recorded has been destroyed
  - Paper, film, or other hard copy media shredded or destroyed so PHI cannot be read or reconstructed.
  - Electronic media cleared, purged, or destroyed consistent with NIST Special Publication 800–88 (Guidelines for Media Sanitization)

Business Associate Agreements

Mandatory Business Associate Assurances	
Scope of permitted data use	Prohibition of secondary uses
Measures against unauthorized access & misuse	Reporting of incidents & unauthorized use
Flow down to subcontractors	Facilitate access, amendment & accounting
Records available to HHS	Comply as if BA were CE
Return/destroy upon completion	Right to terminate for violation

Optional Business Associate Terms	
Use & disclosure for BA management & administration	Data aggregation

Minimizing Uses and Disclosures

- Minimum necessary rule: Only essential data may be used or disclosed
  - Use only de-identified information if feasible
  - HIPAA still applies if researcher conducts the de-identification
- Limited Data Sets
  - Special mechanism if indirect identifiers are needed for research
  - Allows retention of dates and additional geo-data
  - Subject to a written Data Use Agreement limiting further use and disclosure

Research Under HIPAA

- PHI can be used and disclosed for research purposes under specified conditions
  - Individual authorization
  - IRB or privacy board approval or waiver of authorization
  - No authorization or waiver required for
    - Limited Data Sets/Data Use Agreement
    - Limited internal work preparatory to research
    - Research using information about decedents
- HIPAA authorization is distinct from informed consent
  - May generally be combined in a single document

Research Under HIPAA

- HIPAA authorization may include permission for future research (e.g., database or repository)

  - "[A]uthorization for uses and disclosures of protected health information for future research purposes must adequately describe such purposes such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research." 78 Fed. Reg. 5612.

Health Data Research Considerations

- Researchers and sponsors are not business associates
  - Except researcher may be BAs if research is conducted as a service to the health care provider or other CE
- Noncompliance by a site can disrupt research and lead to liability for use of data without proper authorization

Parties in research still have an interest in other parties' compliance:
Scope & content of HIPAA authorizations for research data
Scope & content of the informed consent used by institution
Confidentiality terms between sponsor & CRO
Assurance that institution is compliant
Ensure that institution's privacy policy notice is not unduly restrictive
Procedures to facilitate accounting of disclosures

Health Data Commercialization

- "Sales" of PHI require individual authorization:

  "a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.''

Non-HIPAA Health Data

- Health information is frequently handled by companies that are neither covered entities nor business associates
  - Researchers that are neither CEs nor BAs
  - Consumer-driven data may have never been PHI (e.g., PHRs)
- FTC regulation and state laws still apply
  - FTC Medical Breach Rule for non-HIPAA PHRs

EU Data Protection Regime

- Most countries have followed a comprehensive rather than sector-specific regulatory model
- European Union's 1995 Privacy Directive
  - Mandates national legislation to implement FIPs for data concerning identifiable persons
  - Distinguishes "controllers" from "processors"
    - Controller "determines the purposes and means of the processing of personal data"
    - Processor conducts operation on personal data "on behalf of the controller"

EU Data Protection Regime

- Implications for transborder data flows
  - Transfers allowed within EU or to countries with “adequate” laws
  - U.S. laws not considered to be adequate
  - Alternative methods to legitimize transfers to the U.S.
    - Consent
    - Safe harbor
    - Model contract/ standard clauses
    - Binding corporate rules
- EU is developing a Data Protection Regulation to replace the Directive with a single EU-wide rule
  - European Commission, Parliament and Council are negotiating terms; agreement expected by end of 2015
  - Implementation possible by 2018

EU Rules Applied to Health Research

- EU regulation may be burdensome for research by U.S. companies that do not already have EU operations subject to data protection requirements
- Use of equipment in the EU is sufficient to confer EU data protection jurisdiction
- Sponsors are generally considered to be controllers or joint controllers with study sites– Sponsors need to:
  - Appoint data protection representative
  - Oversee compliance by their processors (e.g., CROs)
  - Implement mechanisms for transferring data to U.S.

Draft EU Regulation: New Pain?

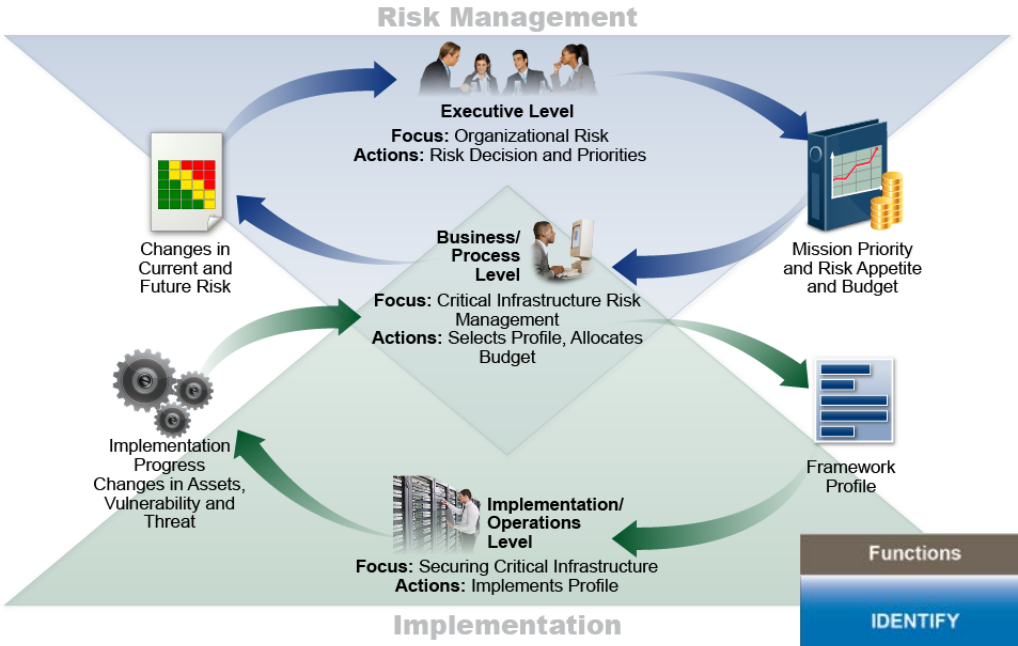
- EU jurisdiction
  - Extraterritorial application to companies with no EU operations
  - Plan for single point of EU regulation might not survive

- Pre-research considerations
  - Mandatory appointment of data protection officer
  - Mandatory PIA and DPA consultation for trials and new research presenting privacy risk
  - Coded data not considered anonymous, but consent may be insufficient if there is a “significant imbalance”

- Restrictions on research
  - Right to be forgotten, including by third party recipients
  - Continued restrictions on outbound data flow
  - Eventual phase-out of U.S. “safe harbor” option?
  - Mandatory breach reporting within 72 hours

- Fines of up to €100 million, or higher based on annual turnover

NIST Cybersecurity Framework v. 1.0



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Data Breaches at Life Sciences and Health IT Companies Growing

Forbes

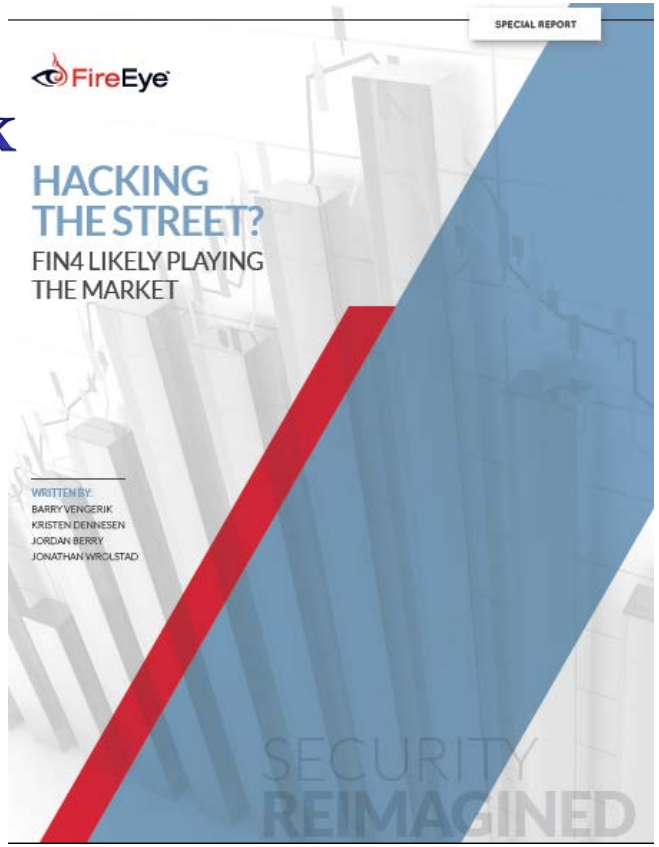
4.5 Million UCLA Health Patients' Data Compromised In Cyber Attack

The New York Times

Indiana Medical Software Company Hack Affected 3.9 Million People

THE WALL STREET JOURNAL.

Community Health Systems Says It Suffered Criminal Cyberattack



Cyber Threat Landscape and Breach Response

BEFORE

INTERNAL THREATS

EXTERNAL THREATS

Hacktivists

Criminals

Espionage

Terrorists

Military

Breach

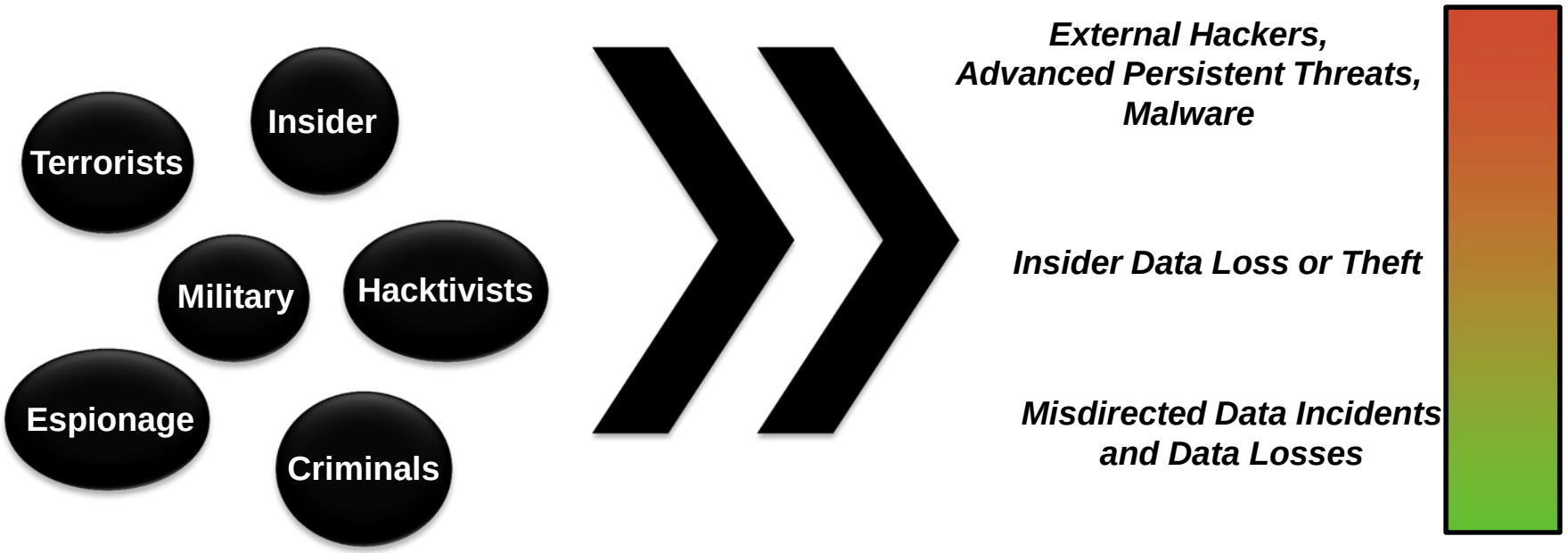
AFTER

- FORENSICS
- CUSTOMERS
- EMPLOYEES AND BOARD
- MEDIA
- LAW ENFORCEMENT
- REGULATORS
- INSURERS
- LEGISLATURES
- LITIGATION

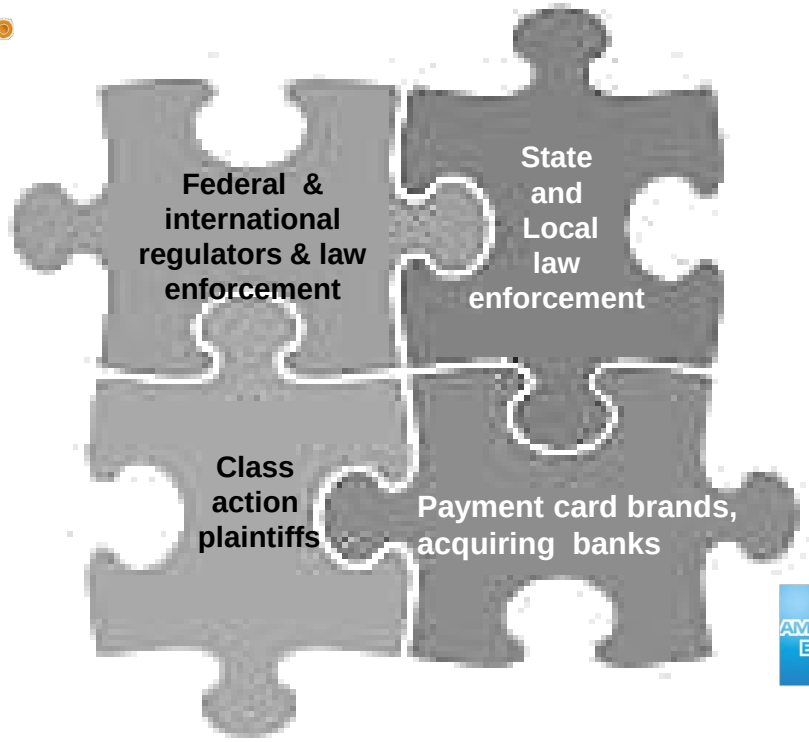
There Will Be A Way In

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

- Robert Mueller, Former FBI Director, 2012 RSA Cybersecurity Conference



Exposure Landscape



Some Lessons from the Field: IT Practices

Overall Management

•Failure to address recommendations from third-party assessments
•Unbalanced risk assessment process

Identity and Access Management

•Lack of control over system administrator credentials
•Use of default passwords for privileged accounts
•Improper/unnecessary access to networks by third-parties

Data Protection

- Lack or failure of encryption
- Incomplete inventory of sensitive data and its locations, leading to insufficient protection for the data

Infrastructure Security

- Improper segmentation
- Failed or insufficient network monitoring
- Unnecessary permissions for connections between severs
- Failure to decommission systems no longer in use
- Unnecessary connection between servers and the external internet
- Failure to deploy purchased network security/monitoring tools

Application Security

- Application patching and updating problems
- Failure to restrict permissions to install unauthorized software
- Failure to audit for known vulnerabilities

Incident Response Planning

Effective data breach response <u>requires</u> pre-breach preparation

- ❑ Written incident response plan:
  - ✓ Identify 24/7 points of contact
  - ✓ Establish clear roles and responsibilities
  - ✓ Provide escalation procedures
  - ✓ Account for different types of incidents
  - ✓ Give guidance on responding to customers, business partners, press, regulators, and others
  - ✓ Reflect notice and reporting requirements
- ❑ Ideally includes tabletop exercises or roleplaying a simulated breach
- ❑ Negotiation of engagement terms with data forensic firm(s)
- ❑ Engagement of other vendors necessary for effective breach response
- ❑ Contingency plans for providing notice to customers

Breach Response: Coordinating Multiple Work Streams

Forensics
Engage firm and manage investigation

Customers

Employees & Board

Media

Legislatures

Law Enforcement

Regulators

Insurance

Litigation

Pick a Leader, and a Team, and Establish High Operational Tempo:

- Manage simultaneous work streams; privileged investigation
- Ensure common and complete understanding of the facts
- Ensure consistent communications to all constituencies

Managing Breach Response

Understand the Incident and Prevent Further Exploitation

- ✓ Conduct a legally privileged investigation
- ✓ What happened and has the breach been stopped
- ✓ How significant is the threat to business
- ✓ First reports are often incorrect/incomplete

Communications Issues

- ✓ Prioritize reputational issues
- ✓ Consider all audiences
- ✓ Consider what you know and do not know
- ✓ What is the core narrative?

Legal Issues

- ✓ Consider legal privilege for all post-breach actions
- ✓ Identify financial control systems ASAP; include in scope of forensic work
- ✓ Address regulators and law enforcement
- ✓ Evaluate legal notification and disclosure requirements
- ✓ Be mindful of potential litigation
- ✓ Insurance

Some Key Takeaways on Breach Preparedness and Response

Pay Attention	• Cyber issues raise legal concerns throughout the enterprise. Be aware of evolving regulatory requirements and expectations.
Be Prepared	• Develop a comprehensive, integrated incident response plan.
Manage Your Response	• Assemble an experienced team—including legal and non-legal components—to ensure breach response is integrated and effective

FDA and Medical Devices

- Guidance on Cybersecurity Considerations in Premarket Submissions for Medical Devices (Oct. 2014)
  - consider cybersecurity during the design phase of medical devices;
  - define and document many components of their cybersecurity risk analysis and management plan as part of the risk analysis required under the Quality System Regulation, including:
    - identification of assets, threats and vulnerabilities,
    - impact assessment of threats and vulnerabilities on device functionality,
    - assessment of the likelihood of a threat or vulnerability being exploited,
    - determination of risk levels and suitable mitigation strategies, and
    - residual risk assessment and risk acceptance criteria;
  - consider appropriate security control methods and provide justification in premarket submissions for controls chosen, such as various methods of
  - limit access to trusted users,
  - build in fail safe and recovery features.

FDA and Medical Devices

- FDA Outreach
  - Emergency Preparedness/Operations & Medical Countermeasures (EMCM) Program
  - October 2014 conference with more than 1300 participants; MITRE website for resources and interaction
  - Medical Device Cybersecurity: Moving the Needle Together (Sept. 2, 2015)
  - Post-market as well as pre-market expectations
    - NIST Framework: Risk management
      - Market Surveillance
      - Cyber hygiene
      - Information-sharing
    - Collaboration with NIST, HHS, and DHS

NIST Guidance: EHRs on Mobile Devices

- NIST SP 1800-1(a-e): Draft Cybersecurity Practice Guide: Securing Electronic Health Records on Mobile Devices
  - maps security characteristics to standards and best practices from NIST and other standards organizations, and to the HIPAA Security Rule
  - provides a detailed architecture and capabilities that address security controls
  - facilitates ease of use through automated configuration of security controls
  - addresses the need for different types of implementation, whether in-house or outsourced
  - provides a how-to for implementers and security engineers seeking to recreate our reference design
- Comments due September 25

Questions?

Jonathan G. Cedarbaum

Partner

(202) 663-6315

Jonathan.Cedarbaum@wilmerhale.com

Barry J. Hurewitz

Partner

(202) 663-6089

Barry.Hurewitz@wilmerhale.com

Brian A. Johnson

Partner and Vice Chair,
Corporate Practice Group

(212) 937-7206

Brian.Johnson@wilmerhale.com

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Boards. Attendees requesting CLE credit must attend the entire program.*