FOLEY HOAG LLP

Driving Business Advantage

Protecting Privacy and Security in the New Health Data Ecosystem:

How to manage your obligations under HIPAA, the HITECH Act and other federal and state data privacy and security laws

Community Health Data Initiative
June 6, 2012

Colin J. Zick
Foley Hoag LLP
(617) 832-1000
www.foleyhoag.com

FOLEY HOAG LLP
Driving Business Advantage

Data Privacy and Security: Why Should It Be a Priority?

- **More federal and state laws, increasing penalties**
- **Theft of consumer information increasing, resulting in** Attorney General settlements, private consumer litigation and harm to brands:
  - **Sony**
  - **TJX/Heartland**
- **Attacks on systems increasing:**
  - **North Korean attacks in 2009 and 2011**
  - **NYSE has suffered several recent incursions**
  - **Stuxnet Worm in Iran's nuclear program**
- **Wikileaks**

FOLEY HOAG LLP
Driving Business Advantage

Laws Impacting Data Privacy and Security

- Federal and 50 State Laws Governing:
  - What information can be collected
  - How it must be stored and secured
  - Under what circumstances it can be shared
  - Under what circumstances it can be disclosed
  - Requirements for responding to data breaches and data losses
  - Penalties for data breaches and data losses

- And then there are the international laws . . .

FOLEY HOAG LLP
Driving Business Advantage

List of U.S. Laws Impacting Data Privacy and Security

- Administrative Procedure Act. (5 U.S.C. §§ 551, 554-558)
- Cable Communications Policy Act (47 U.S.C. § 551)
- Cable TV Privacy Act of 1984 (47 U.S.C. § 551)
- Census Confidentiality Statute (13 U.S.C. § 9)
- Children's Online Privacy Protection Act of 1998 (15 U.S.C. § 6501, et seq., 16 C.F.R. § 312)
- Communications Assistance for Law Enforcement Act of 1994 (47 U.S.C. § 1001)
- Computer Fraud and Abuse Act, as amended by the USA PATRIOT Act (18 U.S.C. § 1030)
- Computer Security Act (40 U.S.C. § 1441)
- Consumer Financial Protection Act of 2010 (Pub. L. No. 111-203, 124 Stat. 1376)
- Criminal Justice Information Systems (42 U.S.C. § 3789g)
- Counterfeit Access Device and Computer Fraud Abuse Act of 1984 (18 U.S.C. § 1030)
- Customer Proprietary Network Information (47 U.S.C. § 222)
- Driver's Privacy Protection Ac (18 U.S.C. § 2721)
- Drug and Alcoholism Abuse Confidentiality Statutes (21 U.S.C. § 1175; 42 U.S.C. § 290dd-3)
- Electronic Communications Privacy Act (18 U.S.C. § 2701, et seq.), aka Stored Communications Act
- Electronic Funds Transfer Act (15 U.S.C. § 1693, 1693m)
- Employee Polygraph Protection Act (29 U.S.C. § 2001, et seq.)
- Employee Retirement Income Security Act (29 U.S.C. § 1025)
- Equal Credit Opportunity Act (15 U.S.C. § 1691, et. seq.)
- Equal Employment Opportunity Act (42 U.S.C. § 2000e, et seq.)
- Fair Credit Billing Act (15 U.S.C. § 1666)

FOLEY HOAG LLP
Driving Business Advantage

List of U.S. Laws Impacting Data Privacy and Security (cont.)

- Fair and Accurate Credit Transactions Act of 2003
- Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.)
- Fair Debt Collection Practices Act (15 U.S.C. § 1692, et seq.)
- Fair Housing Statute (42 U.S.C. §§ 3604, 3605)
- Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)
- Freedom of Information Act (5 U.S.C. § 552) (FOIA)
- Genetic Information Nondiscrimination Act (P.L. 110-233, 122 Stat. 881)
- Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, et seq.)
- Health Insurance Portability and Accountability Act (Pub. Law No. 104-191 § §262,264: 45 C.F.R. § §160-164))
- Health Research Data Statute (42 U.S.C. § 242m)
- HITECH Act (Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5)
- Mail Privacy Statute (39 U.S.C. § 3623)
- Paperwork Reduction Act of 1980 (44 U.S.C. §3501, et seq.)
- Privacy Act of 1974 (5 U.S.C. § 552a)
- Privacy Protection Act (42 U.S.C. § 2000aa)
- Right to Financial Privacy Act (12 U.S.C. § 3401, et seq.)
- Tax Reform Act (26 U.S.C. § §6103, 6108, 7609)
- Telecommunications Act of 1996 (47 U.S.C. § 222)
- Telephone Consumer Protection Act of 1991 (47 U.S.C. § 227)
- U.S.A. Patriot Act (Pub. L. 107-56) (bill extending three anti-terrorism authorities signed 02/25/11)
- Video Privacy Protection Act of 1998 (18 U.S.C. § 2710)
- Wiretap Statutes (18 U.S.C. §2510, et seq.; 47 U.S.C. § 605)

FOLEY HOAG LLP
Driving Business Advantage

BASIC TEMPLATE FOR FEDERAL AND STATE PRIVACY LAWS

- Define the type of “non-public personal information” (“NPI”) that is being regulated
- Provide that NPI must be protected from disclosure to unauthorized holders unless “anonymized” or “aggregated”
- Requires the development, implementation, maintenance and monitoring of comprehensive, written information security programs:
  - Collect only needed information
  - Retain only as long as necessary
  - Provide access only to those with a legitimate business purpose
  - Implement specific administrative, physical and electronic security measures to ensure protection
- Require prompt notice to individuals whose NPI is compromised
- Provides for the imposition of penalties for breaches by NPI custodians
- Requires the disposal of personal information in such a way that it cannot be read or reconstructed after disposal

For example, the Massachusetts Data Security Law

- Most recent law in the area of data privacy and security – Mass. Gen. L. ch. 93H.
- Enacted after the TJX data breach was made public.
- Intended to protect Massachusetts residents from identity theft.
- Applies to any business entity that owns, licenses, maintains or stores the **"personal information"** of a Massachusetts resident, wherever that data is.

FOLEY HOAG LLP
Driving Business Advantage

What is "Personal Information" under the Massachusetts law?

"Personal Information" is:

- A person's first name and last name (or first initial and last name) **PLUS** any **one** of the following:
  - Social Security number
  - Driver's license number (or other state issued ID card number)
  - A financial account number, or credit or debit card number, with or without any required security code, access code or PIN that would allow account access

FOLEY HOAG LLP
Driving Business Advantage

Federal Law: HIPAA and the HITECH Act

HIPAA was passed in 1996; it applies to “protected health information” or “PHI.”

PHI includes what physicians and other health care professionals typically regard as a patient's personal health information, such as information in a patient's medical chart or a patient's test results, as well as an individual's billing information for medical services rendered, when that information is held or transmitted by a covered entity. PHI also includes identifiable health information about subjects of clinical research gathered by a researcher who is a covered health care provider.

HIPAA has three primary regulatory elements related to health information:

- Privacy regulations – April 2003
- Transactions and code set regulations –October 2003
- Security regulations – April 2005

The HITECH Act of 2009 modifies the privacy and security requirements and provides a "floor" for notification requirements regarding any security breach of patients' "unsecured protected health information."

FOLEY HOAG LLP
Driving Business Advantage

Does HIPAA Apply To You?

- HIPAA applies directly to “covered entities”
- What kinds of businesses are “covered entities”?
  - Health care providers
  - Health plans
  - Health care clearinghouses

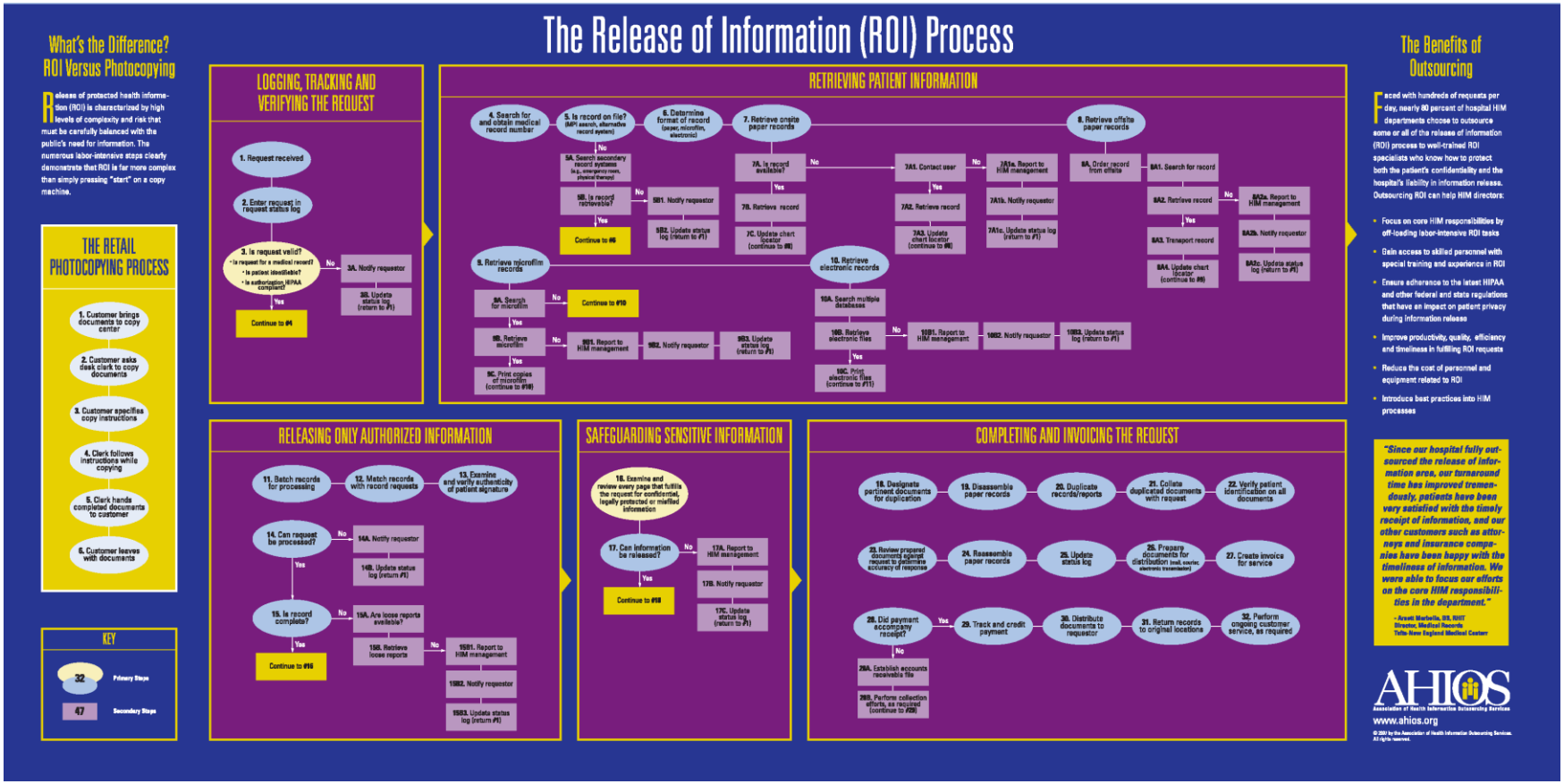
FOLEY HOAG LLP
Driving Business Advantage

HITECH ACT

- In March 2010, fulfilling what Senator Edward Kennedy described as “the great unfinished business of our society,” comprehensive health reform was adopted in the Patient Protection and Affordable Care Act and the Health Care and Education Reconciliation Act.
- But, a year before, HIT changed first, via the Health Information Technology for Economic and Clinical Health Act (the “HITECH” Act), part of the American Recovery and Reinvestment Act of 2009 (“ARRA”).

FOLEY HOAG LLP
Driving Business Advantage

Release of Information Can Be Complicated!



FOLEY HOAG LLP
Driving Business Advantage

Areas Addressed by the HITECH Act and Related Regulations

- Guidance on technology/methods to render PHI unusable in the event of a breach
- Dealing with data breach, particularly breach notification
- Extension of privacy and security provisions to business associates
- Enforcement

FOLEY HOAG LLP
Driving Business Advantage

Guidance on Technology/Methods to Render PHI Unusable in the Event of a Breach

- When issued: April 17, 2009
- What is it? Guidance specifying the technologies and methodologies acceptable to render PHI, which is stored on paper or in electronic format, unusable, unreadable, or indecipherable to unauthorized persons.
- What does it mean? If you follow these standards for encryption, then you are within safe harbor and they would not be required to give the prescribed notification in the event of a breach.
- What do you have to do: Render PHI "unusable, unreadable, or indecipherable" to unauthorized individuals, or make notice for all breaches.

FOLEY HOAG LLP
Driving Business Advantage

Federal Breach Notification Rules

- **When issued?** The interim final regulations were published in the Federal Register on August 24, 2009
- **What is it?** Breach notification for breaches from September 23, 2009 onward. No sanctions until February 22, 2010.
- **What does it mean?** HITECH defines "breach" as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."
- **What do you have to do?** HITECH requires a covered entity to notify each individual "whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed" due to the breach. Here's the form: http://transparency.cit.nih.gov/breach/index.cfm

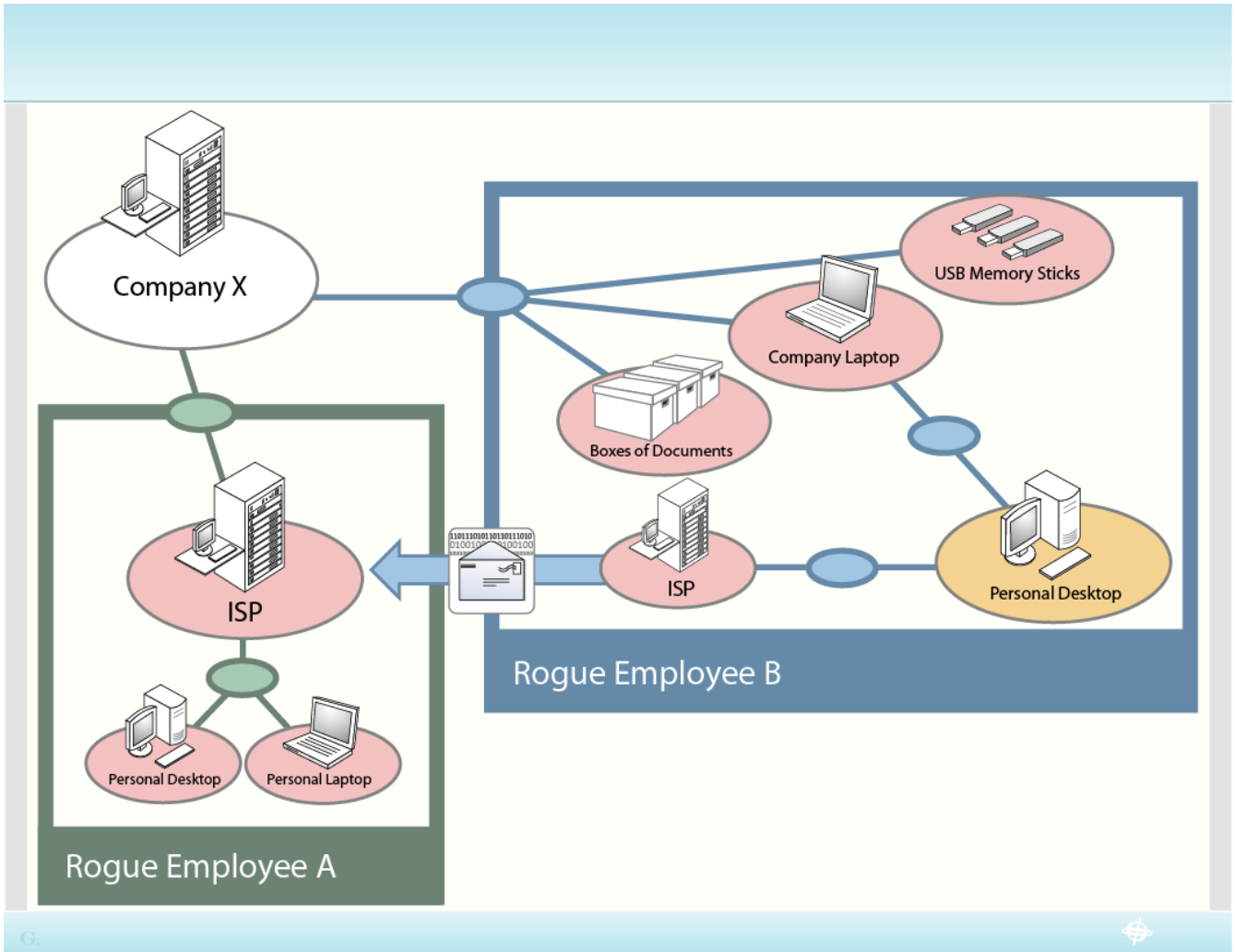
FOLEY HOAG LLP
Driving Business Advantage

The Number and Size of Breaches Continues to Rise

- At the end of February, OCR posted on its website a list of HIPAA "covered entities" that have reported breaches of unsecured health information affecting more than 500 individuals. OCR's posting showed 35 health data breaches that impacted over 700,000 individuals (with individual breaches ranging in size from 359,000 individuals, due to the theft of a laptop to 501 individuals impacted by the theft of a portable USB device). It's now over 100 and they haven't updated the list since June.
- This posting by OCR was required by the August 2009 Interim Final Rule, which was issued pursuant to the HITECH Act. In particular, § 164.408 of this breach notification interim final rule implements § 13402(e)(3) of the HITECH Act. The rule became effective September 23, 2009.
- Under this rule, breaches that affected 500 or more individuals must be reported to OCR within 60 days, via an OCR online notification form. Training materials and related guidance on breach notification can be found on the OCR web site.

FOLEY HOAG LLP
Driving Business Advantage

Anatomy of a Data Breach



FOLEY HOAG LLP
Driving Business Advantage

Common Data Breach Scenarios

- Accidental Breaches
- Faithless Employee/Ex-Employee
- Hackers & Thieves / Organized Crime
- Competitive Espionage

FOLEY HOAG LLP
Driving Business Advantage

Legal Framework – A subset

Customer Privacy Laws

- Federal and state identity theft laws and regulations
  - Requiring customer notice
  - Requiring information security programs
- HIPAA / Medical information regulation
- Gramm Leach Bliley / Financial information regulation
- Regulations for specific industries (e.g., FCC CPNI Regulations)
- Laws governing specific information (e.g., Social Security number statutes)
- Negligence / Consumer protection laws

Authorized Use Statutes

- Computer Fraud & Abuse Act (CFAA)
- Electronic Communications Privacy Act (ECPA)
- Stored Communications Act (SCA)

Surveillance / Information Security Law

- Federal & State Wiretapping Statutes
- Invasion of Privacy

Property Law

- Larceny / Conversion
- Trade Secrets
- Copyright / Digital Millennium Copyright Act (DMCA)

FOLEY HOAG LLP
Driving Business Advantage

Preparing for and Responding to a Breach

- Compliance / developing information security programs
- Incident response and investigation
- Breach notification and resolution
- Litigation
- Government Investigation

FOLEY HOAG LLP
Driving Business Advantage

Federal HIPAA Settlements and Penalties

- Resolution Agreement with Providence Health & Services--July 16, 2008: $100,000
- Resolution Agreement with CVS Pharmacy, Inc.--January 16, 2009: $2.25 million
- Resolution Agreement with Rite Aid Corporation--July 27, 2010: $1 million
- Resolution Agreement with Management Services Organization Washington, Inc.--December 13, 2010: $35,000
- Civil Money Penalty issued to Cignet Health of Prince George's County, MD--February 4, 2011: $4.3 million
- Resolution Agreement with General Hospital Corp. & Massachusetts General Physicians Organization, Inc.--February 14, 2011: $1 million

FOLEY HOAG LLP
Driving Business Advantage

Things to look for in 2012:

- Increased federal regulation in array of "hot" areas:
  - Cybersecurity
    - Malicious code directed at military and manufacturing targets
    - Cyber-criminal incursions focused on theft of intellectual property and other "industrial espionage"
  - Comprehensive breach notice
  - File-sharing risk control
  - Subjecting the SEC to Dodd-Frank Wall Street reform style FOIA obligations; amending SEC filings to require cyber-breach/cyber-risk disclosures
- Battle within government to see who regulates the area
- Increased government focus on national security aspects of security and privacy
- Increased corporate focus on internal cyber security programs
- More security breaches

FOLEY HOAG LLP
Driving Business Advantage

Potential New Federal Legislation

On March 16, the Obama Administration called for enactment of a consumer privacy bill of rights.

- Congressman Cliff Stearns (R-FL) is reworking the online privacy legislation which he originally helped draft with former Congressman Rick Boucher (D-VA) last year. His bill is expected to seek to:
  - compel websites to notify users about the collection and use of their personal data, and
  - users would have to opt in before websites could collect certain particularly sensitive information, including health or financial data.
- Industry believes that the legislation would hamper the provision of free online content supported by ad revenue.
- Privacy advocates say it would not go far enough protect consumers.

FOLEY HOAG LLP
Driving Business Advantage

Potential New Federal Legislation (cont.)

- According to Hillicon Valley, Rep. Jackie Speier (D-Calif.) will shortly introduce an online privacy bill directing FTC to implement a "do not track" regime applicable to online advertisers (this although public comments to the FTC report supporting such a measure, *Protecting Consumer Privacy in an Era of Rapid Change*, are still coming in). Rep. Speier's bill is said not to include any safe harbor provision.

- In contrast, the privacy bill forthcoming from Rep. Bobby Rush (D-Ill.) will not include a "do not track" mandate, but is anticipated to be very similar to the bill he proposed in 2010 that provided a safe harbor to marketers participating in a FTC-approved, self-regulatory "Choice Program." Any approved "Choice Program" would, true to its name, be required to provide users with a robust set of options concerning the collection and use of their information.

FOLEY HOAG LLP
Driving Business Advantage

Colin J. Zick is a partner in Foley Hoag LLP's Administrative and Litigation practice groups. His work has had a particular emphasis on compliance issues related to health care providers, as well as pharmaceutical and medical device companies. This compliance work includes helping clients establish and maintain effective compliance programs. He counsels clients on issues involving information privacy and security including HIPAA, and state and federal data privacy and security laws.

Colin also defends clients in disputes alleging kickbacks, overpayments, and billing and coding problems, and represents clients before various state health care licensing and regulatory entities. Colin serves as the Chair of the Lex Mundi Health Care Industries Practice Group and Co-Chair of the Boston Bar Association's Health Law Section. He has been ranked by CHAMBERS USA as one of Massachusetts' leading health care lawyers and selected by his peers as a Massachusetts "Super Lawyer" since 2004.

Colin can be reached at (617) 832-1275, czick@foleyhoag.com.

FOLEY HOAG LLP
Driving Business Advantage

RESOURSES

- HHS OCR: http://www.hhs.gov/ocr/privacy
- FTC: http://www.business.ftc.gov/privacyandsecurity
- Department of Commerce: http://www.commerce.gov/node/12471
- Advanced Cyber Security Center: http://www.massinsight.com/initiatives/cyber_security_center/
- Our blog: http://www.securityprivacyandthelaw.com

Thanks to my colleagues Ara Gershengorn and Sarah Altschuller who helped me assemble this presentation.