FOLEY HOAG LLP
Driving Business Advantage

Data Security and Privacy for Medical Device, Pharmaceutical and Life Sciences Companies:

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

March 29, 2011

Colin J. Zick
Ara B. Gershengorn
Sarah Altschuller
Foley Hoag LLP
(617) 832-1000
www.foleyhoag.com

1

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:**
  - **TJX/Heartland**
    - Attorney General settlement
    - Private consumer litigation
    - Harm to brand
- **Attacks on systems increasing:**
  - **North Korean attack in 2009**
    - Treasury Department and Federal Trade Commission Web sites were shut down by the software attack, which lasted for days.
  - **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)

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.

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
- Pharmaceutical and medical device companies are typically not covered entities.

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”).

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

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

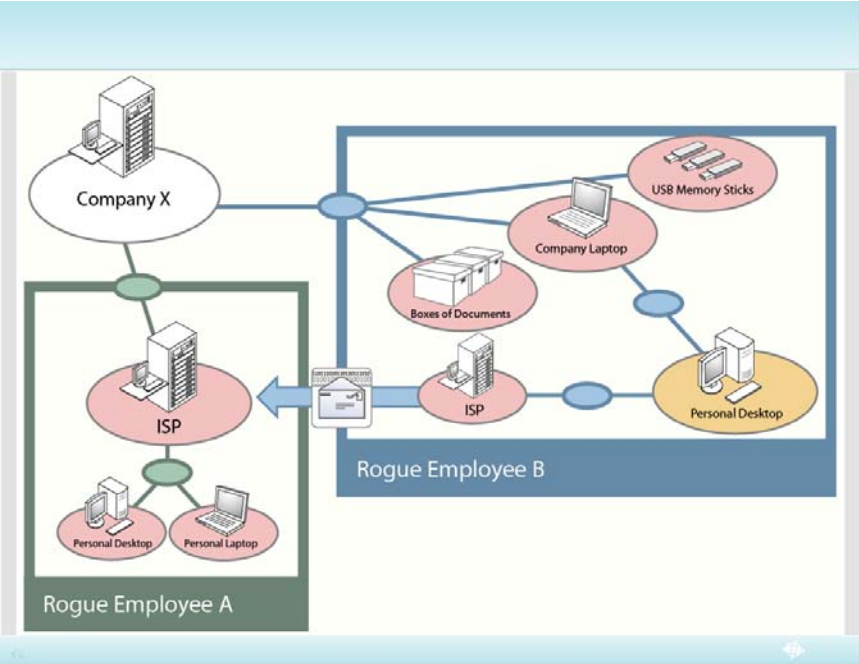
FOLEY HOAG LLP
Driving Business Advantage

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 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

Dealing with a disloyal employee involved in a data breach

- Identifying the bad actors:
  - Anonymous or indentified?
    - "John Doe" lawsuit
  - Acting alone or conspiracy?
  - Current or ex-employee?
    - Addressing employment considerations
  - Are competitors involved?
- Tools:
  - Non-competition/non-solicitation agreements
  - Non-Disclosure Agreements (NDAs)
  - Use of computer company regulations
  - Forensic analyses

FOLEY HOAG LLP
Driving Business Advantage

Dealing with a disloyal employee involved in a data breach (cont.)

- Potential causes of action:
  - Breach of contract/fiduciary duty
  - Misappropriation
  - Consumer protection (unfair business practices) statutes
  - Tortious interference with business relations
  - Federal violations (CFAA or SCA)
  - Commercial defamation
  - Other parties harmed?
- Remedies:
  - Temporary restraining order, preliminary injunction
  - Impounding computers
  - Order to return materials
  - Money damages

FOLEY HOAG LLP
Driving Business Advantage

HIPAA Business Associate Rule

- A Covered Entity may not disclose PHI to a Business Associate without "satisfactory assurance" that the PHI will be appropriately safeguarded, *i.e.*, a written contract with specific provisions
- The rule does not apply to disclosures.
  - By a Group Health Plan, Health Insurance Issuer or HMO to the plan sponsor if the plan document and certification requirements are met
  - By a health plan that is a governmental program (under limited circumstances)

FOLEY HOAG LLP
Driving Business Advantage

HITECH Privacy Rules for Business Associates

- When issued? July 8, 2010
- What is it? Extending to business associates many of the requirements in the Privacy Rules:
  - Establishing new limitations on the use and disclosure of protected health information for marketing and fundraising purposes
  - Restricting the disclosure of PHI) to health plans; expanding individuals' rights to access their information
- What does it mean?
  - HHS's proposed rules confirm the extension of HIPAA privacy and security rules to BAs (essentially making "business associates" into "covered entities.")
  - The proposed rule would add an addition circumstance to the existing two circumstances in current regulations where such authorization is necessary. Currently, authorization is required for (1) most uses and disclosures of psychotherapy notes; and (2) uses and disclosures for marketing. The third circumstance added by the HITECH Act – the sale of PHI – would require a covered entity (or business associate) to obtain authorization for disclosure of PHI that is in exchange for director or indirect remuneration, unless a specified exception applies.
- What do you have to do? HHS intends to provide covered entities and business associates with 180 days beyond the effective date of the final rule to come into compliance with "most of the rule's provisions."

HITECH Security Rules for Business Associates

- When issued? July 8, 2010
- What is it? Extending to business associates many of the requirements in the Security Rules
- What does it mean? HHS proposes a number of changes to the Security Rule including technical modifications as well as modifications to references to business associates.
- **What do you have to do?** HHS intends to provide covered entities and business associates with 180 days beyond the effective date of the final rule to come into compliance with "most of the rule's provisions."

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

Preserving Private Information and Avoiding Privacy Violations when Conducting Clinical Trials

The HIPAA Privacy Rule permits a covered entity to use or disclose PHI for research under the following circumstances and conditions:

- If the subject of the PHI has granted specific written permission through an authorization that satisfies § 164.508;
- For reviews preparatory to research with representations obtained from the researcher that satisfy § 164.512(i)(1)(ii) of the Privacy Rule;
- For research solely on decedents' information with certain representations and, if requested, documentation obtained from the researcher that satisfies § 164.512(i)(1)(iii) of the Privacy Rule;
- If the covered entity receives appropriate documentation that an IRB or a Privacy Board has granted a waiver of the Authorization requirement that satisfies § 164.512(i);
- If the covered entity obtains documentation of an IRB or Privacy Board's alteration of the Authorization requirement as well as the altered Authorization from the individual;
- If the PHI has been de-identified in accordance with the standards set by the Privacy Rule at § 164.514(a)-(c) (in which case, the health information is no longer PHI);
- If the information is released in the form of a limited data set, with certain identifiers removed and with a data use agreement between the researcher and the covered entity, as specified under § 164.514(e);
- Under a "grandfathered" informed consent of the individual to participate in the research, an IRB waiver of such informed consent, or Authorization or other express legal permission to use or disclose the information for research as specified under the transition provisions of the Privacy Rule at § 164.532(c).

Source: NIH – Clinical Research on the HIPAA Privacy Rule

FOLEY HOAG LLP
Driving Business Advantage

Preserving Private Information and Avoiding Privacy Violations when Conducting Clinical Trials (cont.)

Authorization for PHI Uses and Disclosures

- An individual's signed permission that allows a covered entity to use or disclose PHI for specified purpose(s) and recipient(s). For research purposes, it may pertain only to a specific research study, not to future, unspecified projects.
- An Authorization differs from an informed consent: permission for a covered entity to use or disclose PHI for a certain purpose versus permission to participate in the research.

Authorization Core Elements

- A description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner
- The names of the persons authorized to make the requested use or disclosure
- The names of the persons to whom the covered entity may make the requested use or disclosure
- A description of each purpose of the requested use or disclosure
- Authorization expiration date or expiration event
- Signature of the individual and date.

Authorization Required Statements

- A statement of the individual's right to revoke the authorization
- Whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on Authorization
- A statement of the potential risk that PHI will be re-disclosed by the recipient and no longer protected by the Privacy Rule.

Source: NIH – Clinical Research on the HIPAA Privacy Rule

FOLEY HOAG LLP
Driving Business Advantage

Social Media and Consumer Marketing: the FTC Approach

- Privacy by design:
  - Incorporate substantive privacy protection into corporate practices from the ground up, such as in data security, collection limits, retention practices and maintaining data accuracy
  - Maintain comprehensive data management procedures throughout life cycle of products and services
- Simplify choices for consumers
- Achieve transparency to users:
  - Shorter, clearer privacy notices
  - Reasonable consumer access to the data they maintain
  - Prominent disclosures and express consent before using data in a materially different manner than claimed when the data was collected
  - Educate consumers

Social Media and Consumer Marketing: the Department of Commerce Approach

- Fair Information Practice Principles (FIPPs)
  - Transparency: Organizations should be transparent and notify individuals regarding collection, use, dissemination and maintenance of personally identifiable information
- FIPPs would be supplemented by "voluntary enforceable industry codes":
  - Relevant multi-stakeholder process for proposing new codes
  - Approved and enforced by FTC
  - Compliance is a safe harbor
- FTC would enforce FIPPs
  - Unclear if there would be federal private rights of action or federal pre-emption

FOLEY HOAG LLP
Driving Business Advantage

Adhering to the E.U. Privacy Directive

- **E.U. Directive 95/46/EC**
  - Addresses the collection, use, processing, and free movement of personal data.
  - Broad definition of "personal data" – "any information relating to an identified or identifiable natural person."
  - Each E.U. member state is required to enact implementing legislation.
  - Raises concerns for European-based companies, U.S.-based companies, and for companies who provide services to companies who are subject to the Directive.
  - Impacts "data controllers", "data processors," and data transfers.

FOLEY HOAG LLP
Driving Business Advantage

E.U. Privacy Directive – Key Points

- **Data controllers**:
  - **Data collected only for "specified, explicit and legitimate" purposes. May not be in excess of what is needed for such purposes.**
  - **Data must be accurate and up to date.**
  - **Data must not be kept in a form that permits identification of the data subjects for any longer than is necessary.**

FOLEY HOAG LLP
Driving Business Advantage

E.U. Privacy Directive – Key Points (cont.)

- **Data Processors**:
  - **Data subject much give unambiguous consent to the processing; or**
  - **Data processing must be necessary:**
    - To the performance of a contract with the data subject;
    - To the performance of a contract to comply with legal obligations of the data controller;
    - To protect vital interests of the data subject;
    - For public interest reasons or the exercise of some official authority; or
    - For the purposes of legitimate interests pursued by the data controller or by third-party recipients of the personal data, provided such interests are not outweighed by the data subject's interests.

FOLEY HOAG LLP
Driving Business Advantage

E.U. Privacy Directive – Key Points

- **Data subjects have certain rights of access to personal data.**
- **Heightened concern about "special categories" data (data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life)**
- **European Commission has undertaken a review of the E.U. data privacy rules. Proposals expected in mid-2011.**

FOLEY HOAG LLP
Driving Business Advantage

E.U. Privacy Directive – Data Transfers

- **Transfers permissible if to country that the European Commission has determined "ensures an adequate level of protection." United States does not qualify.**
- **Other means**:
  1) **U.S. Department of Commerce/European Commission: Safe Harbor Framework allows for data transfers to certified organizations.**
     - Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission may participate in the Safe Harbor Scheme and may self-certify directly on the Department of Commerce's website.
     - Organizations that decide to participate in the Safe Harbor framework must comply with the Safe Harbor's requirements and publicly declare that they do so.
  2) **Standard contractual clauses to safeguard data transfers.**
  3) **Article 26 Derogations (*i.e.,* data subject has given his consent unambiguously to the proposed transfer).**
  4) **Intra-corporate transfers when multinational has adopted Binding Corporate Rules ("BCRs")**

FOLEY HOAG LLP
Driving Business Advantage

U.S./E.U. - Safe Harbor Framework

- **Safe Harbor requires organizations to comply with seven data privacy principles:**
  - **1) Notice**
  - **2) Choice**
    - **Opt-in for sensitive information that may be disclosed to third party, or that may be used in manner other than for purpose for which it was originally collected.**
  - **3) Onward transfer**
  - **4) Access**
  - **5) Security**
  - **6) Data integrity**
  - **7) Enforcement**

FOLEY HOAG LLP
Driving Business Advantage

Things to look for in 2011:

- 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

The Federal Government is Increasingly Focused on This Issue

- In its 2012 Pentagon budget request, the Obama administration designated $2.3 billion to strengthen Department of Defense cyber security operations, including activities of the Pentagon's new Cyber Command and half a billion dollars for new cyber technology research. These figures do not include the growing spending on "black" cyber security activities, embedded within the approximately $80 billion annual intelligence budget.
- The Departments of Commerce, Defense, Homeland Security, Justice, and State are all actively developing cyber security initiatives.
  - On February 16, 2011, Secretary Clinton appointed Christopher Painter to head the new Office of the Coordinator for Cyber Issues, which will coordinate cyber security and other cyber issues across the Department and with other agencies.
  - On February 17, 2011, Sen. Jos. Lieberman reintroduced a comprehensive cyber security bill designed to protect the security of critical U.S. networks and communications system.
  - The Pentagon's cyber bureaucracy alone will soon include more than 40,000 personnel under the supervision of Cyber Command.

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

Presenter Biographies

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 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, state and federal data security laws, and the FTC Red Flag Rules. 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 North America Regional Vice-Chair of the Lex Mundi Health Care Industries Practice Group and Co-Chair of the Boston Bar Association's Health Law §. 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" from 2004 through 2010. He can be reached at (617) 832-1275, czick@foleyhoag.com.

FOLEY HOAG LLP
Driving Business Advantage

Presenter Biographies

Ara Gershengorn, a Foley Hoag partner, brings extensive courtroom experience to her work at Foley Hoag, both trial and appellate, civil and criminal. At Foley Hoag, she has been involved in several internal corporate investigations regarding data breaches and related mitigation efforts. She also has defended clients in government investigations at the federal and state level, as well as in civil litigation proceedings. In so doing, she relies on her prior government experience as a federal prosecutor and civil appellate counsel. Prior to joining Foley Hoag, Ara was an Assistant United States Attorney where she successfully prosecuted criminal jury trials. She also conducted investigations of fraud, tax crimes, and healthcare and securities law violations, as well as drug and violent crime offenses. Ara also briefed and edited dozens of criminal and immigration matters in the federal court of appeals, and argued before the U.S. Court of Appeals for the Third Circuit in cases involving significant sentencing and tax issues. She can be reached at (617) 832-1260, agershengorn@foleyhoag.com.

FOLEY HOAG LLP
Driving Business Advantage

Presenter Biographies

Sarah Altschuller has been a member of Foley Hoag's Corporate Social Responsibility (CSR) practice since 2003. In this role, Sarah advises a wide range of multinational companies regarding the development and implementation of CSR strategies, policies, and procedures, including data privacy, security and breach issues. She provides counsel regarding corporate interactions with socially responsible investors, and advice on stakeholder engagement with local communities, host governments, and non-governmental organizations. She also conducts site-level human rights and labor rights impact assessments, as well as due diligence efforts. Sarah's in-depth practical experience includes post-law school studies at North South University in Dhaka, Bangladesh (2002–2003), where she conducted research on how changing international trade regulations impact the country's garment sector. Before entering law school Sarah conducted social research on publicly-traded domestic and international companies at KLD Research & Analytics, a socially responsible investment firm, currently part of RiskMetrics Group. He can be reached at (202) 261-7387, saltschuller@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