The Continuing Nightmare of Data Breach and Privacy Risks and Regulations: Increasing Risks, New Regulations and Changing Deadlines

Theodore P. Augustinos
Partner
Hartford, Connecticut

Laurie A. Kamaiko
Partner
New York, New York

David S. Szabo
Partner
Boston, Massachusetts

EDWARDS ANGELL PALMER & DODGE

Agenda

1. The significance of data breach issues
2. Personal information: The regulatory and legal landscape of data security requirements
    a. Types of requirements – Pre and post breach
    b. State
    c. Federal
    d. Industry standards
    e. Contractual requirements
    f. Common law
    g. International Issues
3. Protected Health Information: HIPAA and HITECH
    a. The specific category of PHI
    b. HITECH
    c. Changes to HIPAA
    d. Penalties and Sanctions
    e. HIPAA breach notification
    f. FTC PHI rule
4. Enforcement and Exposure Issues
5. Potential Insurance Issues

EDWARDS ANGELL PALMER & DODGE

Data Breaches Are Everywhere: Some Nightmare Statistics of 2008

- U.S. data breaches rose 47% from year before with 656 reported breaches
- 285 million records were reportedly compromised, more than prior 4 years combined
- Mean number records per breach was 4.5 million/median was 37,847 per breach
- 98% of records compromised were of payment cards
- Intellectual Property theft rose to five-year high
- Reports of insider theft doubled to nearly 16% of breaches
  - Some studies attribute 20% to insiders
- Total average cost per breach was reportedly $202 per record
- Lost business reported to account for 69% of breach costs, or $139 per record compromised, averaging $4.9 million per company breached
- 87% of breaches reportedly could have been avoided if reasonable security controls had been in place at time

EDWARDS ANGELL PALMER& DODGE

2009

- 85% of businesses surveyed experienced a data breach (up from 60% in 2008 study)
- Already exposing over 220 million records, 437 Reported breaches as of November 17, 2009

Medical/Healthcare	- 13.3% of breaches	- 4.5% records (9.8 million)
Banking/Credit/Financial	- 13.8% of breaches	- 59% records
Educational	- 15.4% of breaches	- 552,548 records
Government/Military (includes states, Housing Authorities, etc.)	- 17.9% of breaches	- 35.9% records (79 million)
Unspecified Business (Insurers, Law Firms, Stores, etc.)	- 39.5% of breaches	- .4% records

EDWARDS ANGELL PALMER & DODGE

What Are Data Breaches

- The Current Focus: Personal Information that can be used for Identity Theft
  - Generally, name plus:

    Credit Card #
    Social Security Number
    Drivers License or Government Issued ID
    Medical Insurance ID Number
    Financial Account Information
  - Basically, personally identifiable financial and health information of individuals
  - Electronic or Paper
- Personal Health Information
- Breaches of Other Confidential Information Also Occur
  - Corporate Information
  - Trade Secrets/Intellectual Property
  - Cyber attacks to disrupt operations
- Causes: Carelessness or Maliciousness

  Insiders, outsiders, third party providers (vendors)

EDWARDS ANGELL PALMER & DODGE

Target Industries

- Financial Institutions
- Universities
- Medical Facilities
- Retailers
- Payment Processors
- Food & Beverage/Hospitality Industry (restaurants, hotels, etc.)
- Law firms
- Government and Defense Industry
- Employers of all kinds
- Any entity with Personal Information on their systems of employees, customers/clients, third parties

EDWARDS ANGELL PALMER& DODGE

Target Industries *(cont.)*

- Insurance Industry Companies Face Exposures

  (Insurers, Brokers, TPAs, MGUs and other agents, reinsurers and vendors)
  - From their own operations
    - Personal Information of employees, insureds, claimants, beneficiaries
    - Applicants (especially life and personal lines)
  - From their insureds with exposures
    - Intended and non-intended coverage
      - First Party
      - Third Party (Defense costs as well as potential indemnity)
    - Coverage disputes as to whether policies issues actually provide coverage for the cost or claim in issue
  - Information from:
    - Employees
    - Insureds
    - Claimants
    - 3rd Party Litigants

EDWARDS ANGELL PALMER& DODGE

How a Company Responds to a Data Breach Can Significantly Affects Customer/Client Retention

- 83% of consumers surveyed reported receiving data breach notification during prior 24 months
  - 63% said notification offered them no direction on steps to take to protect themselves and as a result:
    - 31% terminated their relationship
    - 57% said they lost their trust and confidence
- Lawsuits based on breaches often include causes of action based on allegations of:
  - Failure to timely and properly notify affected individuals
  - Result and damages

EDWARDS ANGELL PALMER& DODGE

The Regulatory and Legal Landscape of Data Security Requirements

- Two Types of State and Federal Requirements
  - Breach Notification
  - Data Security
- State Statutes and Regulations
  - Many have data protection requirements
    - Creation of privacy policies for Personal Information
    - Proper record disposal
    - Some mandate security procedures
  - 45 States plus DC, PR and VI require data breach notification
    - To affected individuals
    - Some state agencies
    - Some to credit reporting agencies
    - Varying requirements

EDWARDS ANGELL PALMER & DODGE

The Regulatory and Legal Landscape of Data Security Requirements *(cont.)*

- New Massachusetts regulation effective 3/1/2010 sets rigorous new standards
  - Applies to any entity with PI of a Massachusetts resident
  - Implementation of comprehensive written information security program
  - Mandatory security procedures, including encryption, for records, especially those with PI that will travel over public or wireless networks
  - Limitations on collection and retention of Personal Information
  - Ensure vendors safeguard Mass. PI in compliance with Regulation
  - Training and education requirements

EDWARDS ANGELL PALMER& DODGE

The Regulatory and Legal Landscape of Data Security Requirements *(cont.)*

- Federal Requirements
  - Gramm-Leach-Bliley Act
    - Privacy standards for financial institutions including insurance companies
  - FTC Red Flag Rules – effective June 1, 2010, with enforcement delayed for many "financial institutions" and "creditors" other than banking institutions
    - Financial institutions and "creditors" with "covered accounts" - broad definitions and scope
    - Requires Identity Theft Prevention Program to identify "red flags" of risk and mitigation
    - Requires approval of company Red Flag Policy by Board or Board Committee with delegated authority
    - Requires regular reporting
  - HIPAA and HITECH (2009 Economic Stimulus Plan)
    - Protects personal health information
    - Requires notification of unsecured information
    - Fines and penalties
  - Federal "Cyber Czar" and proposals for additional federal regulations

Industry Standards

- Payment Card Industry Data Security Standards (PCI DDS)
  - Data security standards applicable to all organizations that hold, process or pass payment cardholder information
  - Fines and Penalties for non-compliance
  - Contractual between card companies, and merchants and service providers
  - Non-compliance can be evidence of negligence

EDWARDS ANGELL PALMER& DODGE

Contractual Requirements

- Vendor Contracts
  - Some imposed by law or regulation (e.g., MA)
- Customer Agreements
  - Privacy policies
    - They can come back to haunt

EDWARDS ANGELL PALMER & DODGE

Common Law

- Common Law rights
  - To privacy of Personal Information
  - To protection of other confidential information
- Requirements under traditional theories of third-party liability and recovery for actual damages/cognizable legal injury

EDWARDS ANGELL PALMER & DODGE

International - Briefly

- EU Stringent Protections of personal information
  - Broad definitions
  - Broad protections, particularly with regard to cross-border transfers of information
  - New procedures being proposed for notification, etc.
- Interesting Issues for International Businesses
  - Employee Data
  - Customer Data
  - Corporate Affiliates

EDWARDS ANGELL PALMER & DODGE

HIPAA and HITECH

- HITECH Act, a part of the American Reinvestment and Recovery Act, made significant amendments to the HIPAA privacy rule, security rule, and enforcement policy.
- HITECH added a new breach notification obligation for covered entities, business associates
- HITECH also put breach notification obligations on vendors of personal health record systems and their contractors.

EDWARDS ANGELL PALMER& DODGE

Some HIPAA Changes

- Rules and penalties now apply directly to business associates
  - Privacy rule
  - Security rule
- States can now enforce HIPAA directly in federal court
- Still no private right of actions, but state courts can look to HIPAA rules for standard of care and duties.

EDWARDS ANGELL PALMER & DODGE

What Are the New HIPAA Penalties?

- Four tiers:
  - $100 per violation up to $25,000 per year
  - $1,000 per violation, up to $100,000 per year
  - $10,000 per violation, up to $250,000 per year
  - $50,000 per violation, up to $1.5 million per year

EDWARDS ANGELL PALMER & DODGE

What Determines Severity?

- If you did not know of the violation, and would not have known if you exercised reasonable diligence, start at the lowest level;
- If the violation was due to reasonable cause and not willful neglect, start at the second level;
- If there is willful neglect but with prompt correction, start at the third level; and
- If there is willful neglect without prompt correction, start at the highest level.
- But, any violation can lead to the highest tier of penalty (the tiers are minimums)

EDWARDS ANGELL PALMER & DODGE

Criminal Sanctions

- A June, 2005 Memorandum from the Office of Legal Counsel appeared to limit enforcement of criminal sanctions to covered entities;
- This triggered a concern that persons stealing PHI from covered entities might escape prosecution

Criminal Sanctions *(cont.)*

- A person . . . shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity . . .and the individual obtained or disclosed such information without authorization. Sec. 13409 of ARRA.
- Criminal penalties can now apply to “any person” who obtains protected health information without authorization.

EDWARDS ANGELL PALMER& DODGE

HIPAA Breach Notification

- Breach notification is required by Section 13402 of HITECH in the event of a data breach of “unsecured” PHI.
- Notice is not needed if the data is Unusable, Unreadable or Indecipherable (i.e. “secured PHI”).
- Notice not needed if the data is not PHI.
- Notice is not needed for limited data sets that have had birth dates and zip codes removed.

EDWARDS ANGELL PALMER& DODGE

What is a Breach?

- Unauthorized acquisition, access, use or disclosure of PHI, which compromises the security or privacy of such information
- Not all violations of either the Privacy Rule or the Security Rule constitute breaches of PHI.

EDWARDS ANGELL PALMER & DODGE

Exceptions

- An unauthorized acquisition, access or use by an employee or individual acting under authority of a CE or BA, in good faith, without further use or disclosure;
- An inadvertent disclosure by an authorized individual at a CE or BA, to another similarly situated person, so long as the PHI is not further acquired, accessed, used, or disclosed; and
- A disclosure to unauthorized person where the CE or BA has a good faith belief that the person would not reasonably have been able to retain such information.

Harm Threshold

- The acquiring, access, use or disclosure of PHI is not a breach if it does not pose a significant risk of financial, reputational or other harm to the individual.
- This requires a risk assessment, taking into account a variety of factors
  - Who acquired the information?
  - Was immediate mitigation carried out?
  - Was data recovered, and can you conclude that it was not further disclosed?
  - Directory information alone probably does not carry a risk of harm, unless there are indicia of the services received.

Risk Assessment

- Burden is on Covered Entity to make a risk assessment
- It must be documented
- A presumption of harm arising from a breach is implied, and burden is on the CE to overcome the presumption before concluding that no notice is required.

Who is Accountable?

- A Covered Entity is accountable for breaches committed by its agents and its business associates.
- A Covered Entity is not accountable for breaches committed by recipients who are neither business associates nor agents, and who had a right to receive PHI, such as:
  - Other covered entities
  - Independent researchers who receive PHI per an authorization or limited data set agreement
  - Government agencies

EDWARDS ANGELL PALMER & DODGE

Discovery of a Breach

- A breach is deemed discovered by a covered entity or business associate on the first day the breach is known to the covered entity; or
- The breach is treated as “known” as of the first day that the covered entity would have known of the breach if it has exercised “reasonable diligence”
- Reasonable diligence is the “business care and prudence expect from a person seeking to satisfy a legal requirement under similar circumstances.”
- Ignorance is not bliss.

EDWARDS ANGELL PALMER& DODGE

Timing of Notice

- Notice must be given promptly, and not later than 60 days of the discovery of the breach.
- A CE should give actual notice to the individual
- BA must notify CE, who in turn must notify the individual.
- Substitute notice permitted where contact information is not available
- Urgent notice by telephone is permitted, but does not replace the need for written notice

EDWARDS ANGELL PALMER & DODGE

Alert the Media and the Secretary

- Required if the breach impacts 500 or more individuals
- Must use a “Prominent Media Outlet”
- The media outlet must have appropriate coverage in light of the location of the individuals (citywide, statewide, etc.)
- Immediate notice to the Secretary for large breaches.
- Breach log to aggregate events involving less than 500 persons, with annual submission to the Secretary.

EDWARDS ANGELL PALMER& DODGE

FTC Breach Notification

- The FTC rule applies to vendors of personal health records and PHR related entities.
- A “PHR related entity” is an entity that offers products or services through the web site of a PHR vendor, offer products or services through the website of a covered entity’s PHR; or access information or send information to a PHR.
- The rule does not apply to covered entities or their business associates.
- The Google Health™ rule?

EDWARDS ANGELL PALMER& DODGE

Notice Obligation

- The notice obligation, timing and content are virtually identical to the provisions of the HIPAA rule, except that the administration of the rule is carried out by the Federal trade Commission, and not by the Secretary of HHS.
- Violations of the FTC Health Data Breach rule are violations of the Federal Trade Commission act, and are unfair and deceptive acts or practices in trade or commerce.
- FTC has a strong record of privacy law enforcement.

Enforcement Triggers *(cont.)*

- Large breaches will be reported in the media
- See www.breachblog.com or www.idtheftcenter.org
- HIPAA enforcement may accompany identify theft prosecutions; investigations under Computer Fraud and Abuse Act, False Claims Investigations, or even Off Label Marketing investigations.

EDWARDS ANGELL PALMER & DODGE

Enormous Exposures For Data Breach

- Potential First Party Costs ($202 per breached record)
  - Forensic costs
    - Determining what happened and how to stop/prevent recurrence
  - Professional advice on requirements triggered and their content
  - Notification costs
    - Content, printing, mailing
    - Call centers and other follow-up
  - Mitigation costs
    - Credit monitoring, etc.
  - Fines and penalties – statutory/regulatory, PCI DSS and other contractual
  - Reputational Harm/Lost business
- Potential Third Party Claims
  - By consumer subject to Identity theft and other data losses
    - Fear of unauthorized use/identity theft without improper use generally insufficient
  - By others with resulting losses
    - Banks, credit unions and other issuers of payment cards that pay for fraudulent transactions and card replacements – claims being made, some dismissed
    - Insurers of those who pay
    - Other merchants, etc. affected by card cancellations and fraudulent transactions

EDWARDS ANGELL PALMER& DODGE

Insurance Policies Potentially Implicated

- Specialty Policies designed to address the risk
  - Cyber Risk, Technology and Privacy Policies
    - Can have sub-limits, exclusions and other limitations on scope of coverage that may apply
- Traditional Policies
  - Claims for coverage/defense may be made under policies not intended to apply to this type of event
  - Whether claim successful depends
    - First party costs harder to prevail
    - Third party claims sometimes trigger defense provisions

EDWARDS ANGELL PALMER & DODGE

Insurance Polices Potentially Implicated *(cont.)*

- First Party
  - Property: is it tangible property
  - Fidelity/Crime: Is it employee crime
  - Factors: Scope of coverage/exclusions
- Third Party – May trigger defense if not ultimately indemnity
  - General Liability
    - Coverage A: Property Damage/Bodily Injury
    - Coverage B: Personal and Advertising Injury
      - "injury … arising out of … oral or written publication in an manner, of material that violates a person's right of privacy"
  - Professional Liability / E&O
  - EPL: Employers Liability
  - D&O

EDWARDS ANGELL PALMER& DODGE

Mitigating Exposures

- Compliance
  - Statutes, regulations and industry standards directed at data protection
- Limiting Access and Retention to
  - What is necessary
  - Who has access
  - Duration of retention
- Training/Awareness
  - In 2008, 88% of all breaches due to negligence not maliciousness
- Vendor/service providers – ensuring data security procedures in place
- Buy in at highest levels
- Common sense precautions
- For all:
  - Recognize, identify and protect against your own exposure to data breach
- For insurers issuing policies:
  - Assessing if policies exposed to data breach claims
  - Wording carefully to effectuate intent
  - Screening/Assessment of insureds

EDWARDS ANGELL PALMER & DODGE

Conclusion

- Data security is an area requiring attention of all employers, financial services firms, and healthcare providers, and anyone else who obtains or maintains personal financial or health information
- Compliance and Prevention are on-going efforts
- The cost of not complying with regulatory requirements include: Legal, Regulatory, Contractual and Reputational Risks
- Data breaches are a growing exposure in frequency and severity with increasing costs
- Insurance industry is exposed as both
  - Entities subject to breaches
  - Insurers of those who incur breaches

EDWARDS ANGELL PALMER& DODGE

Conclusion *(cont.)*

With questions or requests for our paper on Data Breach and Privacy Risks and Regulations, contact:

Theodore P. Augustinos, Partner
20 Church Street
Hartford, CT 06103
taugustinos@eapdlaw.com
860.541.7710

Laurie A. Kamaiko, Partner
750 Lexington Avenue
New York, NY 10022
lkamaiko@eapdlaw.com
212.912.2768

David S. Szabo, Partner
111 Huntington Avenue
Boston, MA 02199
dszabo@eapdlaw.com
617.239.0414

EDWARDS ANGELL PALMER & DODGE