EPSTEIN
BECKER
GREEN


# Privacy & Security Crash Course: What Am I Allowed to Do With My Data?

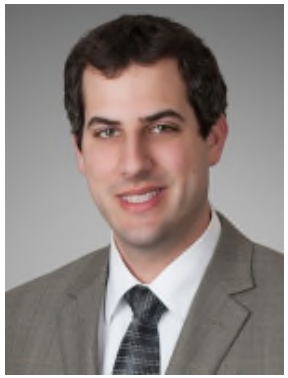
June 9, 2015

This presentation has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal, state, and/or local laws that may impose additional obligations on you and your company.

Cisco WebEx can be used to record webinars/briefings. By participating in this webinar/briefing, you agree that your communications may be monitored or recorded at any time during the webinar/briefing.

Attorney Advertising

# Presented by




**Evan J. Nagler**

Associate

enagler@ebglaw.com

202-861-1878






EPSTEIN BECKER GREEN

# What do data restrictions look like in the USA?


- Sectoral approach
  - Healthcare: HIPAA
  - Financial/Banking: GLB Act, FCRA
  - Consumers: FTC Act
  - Children: COPPA

- Contrast: EU – standardized approach
  - Data Protection Directive
  - "Safe Harbor" for US companies

# What do I need to do before I collect data?


- As appropriate, publish a Privacy Policy
  - FTC requirement for websites collecting data
  - Do not change Privacy Policy without adequate notice
- Healthcare Notice of Privacy Practices required by HIPAA
- Financial Notice of Privacy Practices required by GLB Act

# What types of data need special treatment?


- Payment card data
- Other financial data
- Social Security numbers
- Health information
- “Sensitive” health information
- Movie rental data

# What if I want to involve a third party?


- Implement appropriate protections in your agreements for data sharing
- GLB: confidentiality of information clauses
- HIPAA: Business Associate Agreements
  - Special provisions required for aggregation and de-identification

# Third parties: contract provisions


- Safeguards
- Breach notification
- Remediation
- Insurance/indemnification
- Oversight/auditing
- Termination
- State law obligations

# What do I think about as a vendor?


- Compliance obligations
  - New laws to consider
- Breach obligations
  - Speed of notification
  - Accountability for response
- Indemnification/Insurance
- Data use rights wanted or needed
  - Special requirements: aggregation, de-identification

# What rights do data subjects have?


- COPPA: parents can see information about child, delete and correct
- GLB: opt out of disclosures
- HIPAA: access, corrections, accounting of disclosures

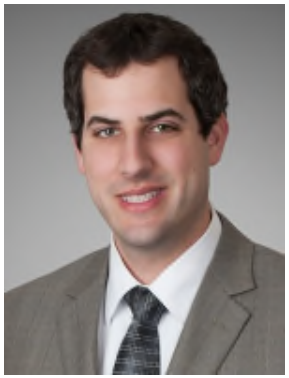
# What security do I need?


- FTC: Behavioral Advertising Principles
  - "Reasonable" security
- FTC: Red Flags Rule
  - "Reasonable" policies and procedures
  - Program to detect and address red flags
- GLB: Safeguards Rule
  - Must have formal information security plan
- HIPAA: Security Rule
  - Specific policies are mandated
  - Some safeguards are required and others are addressable

# How do I dispose of data I no longer need?


- FTC Disposal Rule: flexible standards
  - Physical information: burn, pulverize, or shred
  - Electronic information: erase media such that information cannot be read or reconstructed
- HIPAA: similar requirements for secure disposal

# Questions?

**Evan J. Nagler**

Associate

enagler@ebglaw.com

202-861-1878





EPSTEIN BECKER GREEN

# Upcoming Webinars

## Privacy & Security Crash Course Series


- Privacy & Security Crash Course: How Do I Do a Risk Assessment?
  June 16, 2015 at 2:00pm – 2:15pm EDT
  Adam C. Solander

- Privacy & Security Crash Course: How Do I Execute a Risk Mitigation Plan?
  June 23, 2015 at 2:00pm – 2:15pm EDT
  Brandon C. Ge

- Privacy & Security Crash Course: Recap – Your Questions Get Answered
  June 30, 2015 at 2:00pm – 2:15pm EDT
  People: Patricia M. Wagner

**To register, please visit:** http://www.ebglaw.com/events/

EPSTEIN
BECKER
GREEN

# Thank you.