



# DATA PRIVACY & SECURITY



# WYATT

WYATT, TARRANT & COMBS, LLP

SEE WHY OUR SUCCESS IS DEFINED BY YOURS AT [WYATTFIRM.COM](http://WYATTFIRM.COM)

LOUISVILLE, KY    LEXINGTON, KY    NEW ALBANY, IN    MEMPHIS, TN    NASHVILLE, TN

Wyatt's Data Privacy & Security lawyers have extensive experience with all aspects of this area of the law. We can help a client evaluate and improve their data privacy & security policies and procedures, conduct training, work with regulators, prepare for an external audit, respond to a breach, and draft and review contracts. We also have litigators well-versed in this area of the law.

## OUR EXPERIENCE

The increased use of technology to access, create, transmit, and store data via the internet and on a variety of mobile devices, and the attendant cyber risks for such data, has led to a corresponding need for legal advice regarding the protection of confidential information. Wyatt's Data Privacy & Security Service Team offers a unique blend of experience to address these needs across multiple economic sectors, public and private, for-profit and not-for-profit. We've assisted clients in protecting the confidential information of their patients, employees, and customers, as well as their sensitive operational or business information.

Our attorneys are experienced with state and federal laws protecting consumer information as well as laws setting forth security requirements for such information. All 50 states in the U.S. have a data breach notification law that is implicated when there is unauthorized access to personal information of a resident (as more particularly defined in each law). Some of these data breach laws also include cybersecurity standards to be followed by those who handle personal information. In addition, several states have separate consumer privacy laws with data security requirements (see, for example, the California Consumer Privacy Act and similar laws passed in Colorado, Virginia and Utah). Those who deal with personal information, whether in paper form or electronically, must stay attuned to the evolving protections for the privacy and security of such information.

Wyatt lawyers regularly assist clients in determining their obligations under both state and federal laws to protect and secure personal information as well as in responding to security incidents that may compromise personal information. We have hands-on experience advising clients in many industries, including healthcare, insurance, finance, education, technology, manufacturing, retail, and professional services.

Matters on which our attorneys have assisted clients regarding data privacy and security include:

- Email spoofing or account compromise, sometimes combined with telephone calls, impersonating a trusted source to commit funds transfer fraud
- Business email compromise/phishing/spoofing (social engineering) leading to a potential or actual data breach
- Developing website and mobile app privacy policies and terms of use
- Advising on response and remediation for data security incidents, including:
  - engaging and working with forensics consultants
  - advice on legal obligations under state and federal laws that may be implicated by the incident
  - preparing breach notifications
  - working with media crisis management consultants
  - working with breach notification vendors to distribute individual notifications, set up call center, and provide identity theft/credit monitoring services
- Preparing multi-state charts for privacy law and data breach notification obligations tailored to the client's business or a specific issue







- Working with government regulators on data breach investigations and audits, including the Office for Civil Rights (OCR) and state attorney generals
- Preparing HIPAA Privacy Rule and Security Rule policies and procedures
- Preparing security incident response procedures
- Advising financial institutions on requirements for customer privacy notification and information security
- Negotiating and drafting technology agreements involving access, creation, transmission or storage of personal information
- Drafting and negotiating privacy and cybersecurity related terms in a wide range of business agreements
- Evaluating the risks involved in sharing information with third parties for marketing, transactional or other business purposes
- Performing data privacy and security due diligence for mergers, acquisitions and other transactions
- Advising on the legal requirements for destroying personally identifiable information
- Advising on a wide variety of workplace issues, including surveillance, confidentiality agreements and termination procedures, among others
- Litigating invasion of privacy and defamation matters

## DATA PRIVACY & SECURITY LAWS

Many privacy protection laws are aimed at consumer protection and carry significant penalties for non-compliance or may lead to financial exposure in the form of government settlements or plaintiff class action lawsuits. Among the privacy laws and regulatory schemes on which we regularly advise clients are the following:

- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Trade Commission (FTC) laws, regulations and guidelines related to privacy, including:
  - FTC Act §5: Unfair and Deceptive Practices
  - Fair and Accurate Credit Transactions Act of 2003 (FACTA) and Red Flags Rule
  - Gramm-Leach-Bliley Act (GLBA)
  - CAN-SPAM Act of 2003
  - Children's Online Privacy Protection Act (COPPA)
  - Personal Health Breach Notice Rule
- State data breach notification laws and regulations
- General Data Protection Regulation (GDPR)
- EU-U.S. Privacy Shield Framework
- U.S. Patriot Act
- Family Educational Rights and Privacy Act (FERPA)
- Video Privacy Protection Act of 2015
- Telephone Consumer Protection Act (TCPA)
- PCI Data Security Standards
- Federal Financial Institutions Examinations Council (FFIEC) cyber security statement





## **DATA PRIVACY & SECURITY BLOG: WYATT HITECH LAW**

The Wyatt HITECH Law blog was created in 2009, soon after the passage of the Health Information Technology for Economic and Clinical Health Act (aka "The HITECH Act"). The HITECH Act led which would lead to an explosion in the volume of personal health information kept electronically and accessible over the Internet. Soon afterward, cyber threats increased in all industry sectors, prompting a new market for cyber liability insurance.

The HITECH Law blog provides our clients with current legal developments regarding the creation, access, collection, maintenance or transmission of confidential information regarding an individual, business or organization in all industry sectors. It focuses on issues related to the privacy and security of confidential consumer and business information in today's "high tech" world.

Wyatt is a full-service regional law firm with offices in Louisville and Lexington, Kentucky; New Albany, Indiana; Memphis and Nashville, Tennessee. Wyatt, Tarrant & Combs, LLP is a member of AdvanceLaw. For more information about Wyatt, please visit [www.wyattfirm.com](http://www.wyattfirm.com).

**We believe that the practice of law requires sound advice, prompt service, vigorous advocacy, thoughtful counseling and attention to detail.**

### **LOUISVILLE.KY**

400 West Market Street, Suite 2000  
Louisville, KY 40202  
Telephone: 502.589.5235

### **LEXINGTON.KY**

250 West Main Street, Suite 1600  
Lexington, KY 40507  
Telephone: 859.233.2012

### **NEW ALBANY.IN**

120 West Spring Street, Suite 300  
New Albany, IN 47150  
Telephone: 812.945.3561

### **MEMPHIS.TN**

6070 Poplar Avenue, Suite 300  
Memphis, TN 38119  
Telephone: 901.537.1000

### **NASHVILLE.TN**

333 Commerce Street, Suite 1050  
Nashville, TN 37201  
Telephone: 615.244.0020