Health Privacy & Security
At a Glance

Health care clients are facing unprecedented cybersecurity and data protection issues. The cyber threat landscape is a constantly changing environment. The ever-changing landscape of risks; federal, state, and local legislation; and multiple regulators and law enforcement agencies involved need constant monitoring.

The myriad avenues to breach include medical devices, electronic health records, payment systems, and connections with patients' outside vendors, as well as the increasing threat of ransomware attacks. Perpetrators with varying motives include nation states looking for intelligence (primarily on government employees), criminal organizations seeking financial gain, and potentially terrorists or other nefarious actors attempting to harm patients.

Hard Facts by the Numbers

- According to a May 2015 report by the Ponemon Institute, cyber-attacks cost the US health care system $6 billion in annual losses with the average data breach costing a hospital $2.1 million
- Between April 2014 and June 2015, losses resulting from ransomware cases amounted to more than $18 million
- In 2014, SANS Institute reported the health care industry is not well-prepared to fight growing cyber threats

  Recent breaches affected:

  - 1.1 million CareFirst customers
  - 11 million BlueCross BlueShield customers
  - 4.5 million Community Health Systems records
- Health care information is worth 10 times more than credit card numbers on the black market and can be used for identity theft or health care fraud, which takes much longer to detect
- There are hundreds of documented attacks on radiology imaging software, video conferencing equipment, routers, and firewalls

Targeted Attacks

Companies Compromised

81% of health care executives say their organizations have been compromised by at least one cyber attack in the past two years

- **13%** of the health care respondents say they've been targeted by external hack attempts about once a day. Another **12%** reported 2 or more attacks each week
- **16%** of respondents say they can't detect in real time if their systems have been compromised

*According to a recent survey of health care providers and health plans by KPMG.

Check List

- ☑ Are employees trained to protect personally identifiable information (PII) and identify potential risks of a cyber threat?
- ☑ Do your agreements include provisions protecting your data?
- ☑ Is there a cybersecurity policy? Is it updated regularly?
- ☑ What is the contingency plan when a breach happens?
  - Legal, public relations, credit monitoring, and technical forensics resources should be on call and under contract.
- ☑ Are regular cyber audits being conducted by outside vendors?
- ☑ What are the responsibilities and liabilities when information technology functions are outsourced?
- ☑ Is there cybersecurity insurance in place?
- ☑ Is there a thorough security risk assessment of IT systems and processes that identifies potential vulnerabilities?
- ☑ Are third party vendors being vetted for cybersecurity fitness?
- ☑ Consider membership to National Health Information Sharing & Analysis Center (NH-ISAC).

Areas of Concern

- Data breach notification
- Health records exchange and security
- HIPAA changes
- Complex regulatory structure
- Liability protections for information sharing
- Encryption and government access to data
- Cross-border data flows and different regulation between US/EU/China
- Evolving state and federal legislation
- Business associates and other vendors

Where Arent Fox Can Help

- Cyber Audits
- Employee training
- Government relations intelligence, advice, and advocacy
- Technology agreements
- Cross border transfer issues
- Privacy and terms-of-use policies
- Strategic planning
- Internal protocols
- Advice and counseling pre-, during, and post-event
- Investigations and litigation
- Best practices
- Cybersecurity insurance

About Arent Fox LLP

Arent Fox LLP, founded in 1942, is internationally recognized in core practice areas where business and government intersect. With more than 400 lawyers, the firm provides strategic legal counsel and multidisciplinary solutions to clients that range from Fortune 500 corporations to trade associations. The firm has offices in Los Angeles, New York, San Francisco, and Washington, DC.

Get more in-depth information by scanning the code at right ▸

Having trouble?
No problem. Visit us online:
www.arentfox.com

Key Arent Fox Contacts

Sarah Bruno
Partner, SF
415.805.7945
sarah.bruno@arentfox.com

Sarah Bruno is a data security partner based in San Francisco, and was one of the co-leaders of the team that handled one of the largest known data breaches in the US. She routinely counsels clients in all areas of data security and privacy, including advising corporations on the internal and external privacy protocols to ensure compliance with local laws, as well as the applicable US laws. She also evaluates and advises on the applicable state requirements related to data privacy and security, as well as the precedent promulgated and enforced by the Federal Trade Commission and State Attorneys General.

Thomas Jeffry
Partner, LA
213.443.7520
thomas.jeffry@arentfox.com

Thomas Jeffry is a partner in Arent Fox's Health Care group. His practice is devoted to business and regulatory compliance, including compliance investigations, corporate integrity programs, and transactions. Tom represents hospital systems and other providers along with managed care organizations in many areas, including mergers and acquisitions, drafting and negotiation of contracts, and fraud and abuse issues. In addition, he has extensive experience in corporate governance, nonprofit tax and antitrust issues related to integrated delivery systems, health information technology, bioethics, privacy and security, and HIPAA Administrative Simplification regulations.