List of Applicable Compliance and Regulation Related Items for HIC Inc.

Federal Compliance Measures

Health Insurance Portability and Accountability Act (HIPPA) – This Act regulates the way in which healthcare data is protected via two Titles: Title 1 protects the healthcare information of those who are transitioning between jobs or are laid-off/released from employment and Title 2, specifically the protection of and transition to electronic healthcare records management and data. Title 2 of the act also specifically calls out the protection of privacy of individual patients and their health information.

Sarbanes Oxley Act (SOX) – Primarily applicable to Public Companies, but applied as "Leading Practice" for private entities this act requires companies to maintain financial records for 7 years and puts in specific data protection and audit protocols to protect against insider financial scandal and fraudulent behavior.

Federal Information Security Management Act (FISMA) – Although not directly applicable to HIC through mandate, much like SOX, this act which is specifically related to Federal Agencies and their conduct related to Information Security, serves as a strong set of leading practices for HIC to review and align to where appropriate.

Gramm Leach Bliley Act (GLBA) – Act specifically related to financial industry operatives in Insurance, Commercial banking and Investment banking. Specific to information security, this act mandates that companies operating in these capacities secure the private information of clients, end-users and customers.

Industry Compliance Measures

Payment Card Industry Data Security Standard (PCI-DSS) – Put in place in 2006 by the Payment Card Industry to standardize the protection of credit and payment card vehicles. This standard includes 12 specific regulations designed to reduce fraud and protect consumer credit card information.

Additional Federal Program Considerations

Patient Protection and Affordable Care Act (PPACA) aka Obamacare – While currently nothing specifically is called out in PPACA related to data and information security, we recommend continual monitoring of developments associated with this relatively new law to ensure that if HIC's business or any sub component of it may be future impacted by ratification of this act, we are prepared to shift and meet any/all compliance requirements.

State Compliance Measures

California Notice of Security Breach Act – Passed in 2003, this law requires HIC (or any company that maintains personal information of citizens of California) is bound by law to notify its patrons in the event there is a cybersecurity breach. Further the law requires that HIC disclose details of the event.

California Assembly Bill 1950 – As an augment to the above, in 2004 the California Assembly passed bill 1950 which requires company's maintaining business relations with California residents also maintain a 'reasonable' level of security and that these measures extend to business partners.

California Law - Health Information Privacy

- **Health Facilities Data Breach - California Health & Safety Code section 1280.15**. This law requires certain health facilities to prevent unlawful or unauthorized access to, or use or disclosure of, a patient's medical information. It sets fines and notification requirements for breaches of patient medical information and requires facilities to report such breaches to the California Department of Public Health.
- **Legal and Civil Rights of Persons Involuntarily Detained - California Welfare & Institutions Code section 5328.** This law provides for the confidentiality of the records of people who are voluntarily or involuntarily detained for psychiatric evaluation or treatment.
- **Medical Information, Collection for Direct Marketing Purposes - California Civil Code section 1798.91**. This law prohibits a business from seeking to obtain medical information from an individual for direct marketing purposes without, (1) clearly disclosing how the information will be used and shared, and (2) getting the individual's consent.
- **Medical Information Confidentiality - California Civil Code sections 56-56.37**. This law puts limits on the disclosure of patients' medical information by medical providers, health plans, pharmaceutical companies, and many businesses organized for the purpose of maintaining medical information. It specifically prohibits many types of marketing uses and disclosures. It requires an electronic health or medical record system to protect the integrity of electronic medical information and to automatically record and preserve any change or deletion.
- **Mandated Blood Testing and Confidentiality to Protect Public Health - California Health & Safety Code sections 120975-121020.** This law protects the privacy of individuals who are the subject of blood testing for antibodies to the probable causative agent of acquired immune deficiency syndrome (AIDS).
- **Office of Health Information Integrity - California Health and Safety Code sections 130200.** This law established the Office of Health Information Integrity in the California Health and Human Services Agency, with the mission of ensuring enforcement of state law on the confidentiality of medical information.
- **Patient Access to Health Records - California Health & Safety Code section 123110** and following. With minor limitations, this law gives patients the right to see and copy information maintained by health care providers relating to the patients' health conditions. The law also gives patients the right to submit amendments to their records, if the patients believe that the records are inaccurate or incomplete.

List of Security Controls to Achieve Minimum Compliance: Policy & Application

- **Authorized & Unauthorized Devices**
- **Authorized & Unauthorized Software**

- **Secure Configs for all Devices in Environment (Patch Management)**
- **Continuous Vulnerability Testing & Remediation**
- **Controlled Use of Admin Privileges**
- **Maint, Monitoring and Analysis of Audit Logs**
- **Email & Web Browser Protections**
- **Malware Defenses**
- **Control & Limitation of Network Ports**
- **Data Recovery Capabilities (DRM & BCM)**
- **Secure configurations of Network Devices (Firewalls, Router & Switches)**
- **Perimeter & Boundary Defenses (IPS/IDS)**
- **Data Protection (At Rest & In Transit)**
- **Controlled Access – Permissions Based**
- **Wireless Access Control**
- **Account Monitoring & Control**
- **Security Skills Assessment**
- **Security Training & Best Practices**
- **Application Software Security**
- **Physical Security**
- **Incident Response**
- **Incident Management**
- **Penetration Testing**
- **Establishment of "Red Team" (Cyber Incident Response Team)**
- **Red Team Exercises (Tabletop & Education Measures)**
- **Middleware, Cloud & Vendor Security Postures**