CAPSICUM GROUP™

Regulatory Compliance – HIPAA and HITECH

The regulations, rules and technologies that govern your data and supporting processes, have become a critical core competence for all companies. Where does this data go, who can view it, and how it is protected are issues of paramount importance.

It's fairly obvious that Health Plans, Health Care Providers and Healthcare Clearinghouses must comply with HIPAA rules. But are you aware that they can equally apply to companies that HIPAA defines as business associates? If you are a data storage company, an accounting firm, a law firm, a temporary employment agency, or even a mobile app developer that does business with a healthcare provider, you may be just as accountable for HIPAA compliance as your client is.

Capsicum has developed a simple yet comprehensive program (Technology Health Check) that will ensure you're compliant with regulations and policies concerning your customers' privacy and personal digital information. Our team can assist healthcare vendors, providers and their associates in understanding and complying with continuous changes and amendments to existing healthcare related regulations.

The recent Health Information Technology for Economic and Clinical Health Act (HITECH Act) offers healthcare providers financial incentives for embracing and using electronic health records (EHR). HITECH means that if you work with any company subject to HIPAA you'll be dealing with much more data. HITECH significantly expands HIPAA Privacy and Security rules, with hefty penalties for violations.

One of the areas affected by the HITECH omnibus rule is the "risk of harm" test for unauthorized use or disclosure of Protected Health Information (PHI). The new Breach Notification for Unsecured PHI rule requires covered entities and business associates to prove that there is a "low probability" that PHI has been breached via a thorough risk assessment that considers such factors as: the nature and extent of the breach, how the disclosure was made and used, whether protected information was actually obtained or used and the extent to which the risk has been mitigated.

Our third party risk assessments (Technology Health Checks) demonstrate whether or not there is a low probability that PHI was breached by taking into account the four factors required by the new HITECH rule. The following is a brief summary of assistance we can provide related to data breach reporting and re-identification risk:

1.) Re-identification risk measurement: We examine the plausible attacks on a data set and the kinds of information that an adversary might use for an attack. We then assign probabilities to the various areas of risk as to whether a record has a probability of being re-identified.

2.) Attack simulations: Using industry recognized tools and methods we can make assumptions about the nature of the attack and simulate the likelihood of records in a database being re-identified.

3.) Actual re-identification attack: We attempt to re-identify records in a data set. This is commonly done when a client has de-identified a data set and wants to independently test if it can be re-identified.

Regulatory Compliance – HIPAA and HITECH

Upon completion of our risk assessment and analysis, clients are provided with an objective third party report which includes our findings. In such instances, reporting (and any associated costs) would not be required as they are found to be in compliance. For customers whose data sets do not meet HIPAA's re-identification risk threshold, they are provided with quantifiable information on their specific risk threshold and the affected data.

You may not have thought you're in the healthcare business or the patient privacy data protection business, but if you have customers in the healthcare business you are subject to the same rules. Auditing your company's HIPAA and HITECH readiness could save you a great deal of disruption and financial loss in the future.

Our regulatory compliance review process is multi-pronged:

- **Assess:** Review current policies, processes and technology to determine applicable regulations and analyze a composite of the organization's requirements.
- **Plan:** Recommend actions, determine risks and benefits, develop estimates for remediation and summarize financial impacts (annualized) and potential ROI.
- **Design:** Develop detailed tasks and technology architecture necessary to execute the compliance program.
- **Remediate:** Articulate and document process changes with relevant controls isolated and technology to be acquired, installed or configured.
- **Monitor/Upgrade:** Follow up with an evaluation on a quarterly or semi-annual basis.
- **Implement Compliance:** Coordinate, consult and provide the appropriate documentation to comply.

Strong compliance is the result of strong processes. Capsicum's expertise in data security and compliance governance is the result of many years of experience and a deep understanding of the rules, old and new. We can help you conduct yearly, quarterly or on the spot audits for compliance. Capsicum takes a leading position in your response to HIPAA and related compliance regulations.