[Company Name]

Texas Medical Records Privacy Act Protected Health Information (PHI) & HIPAA Training Program Manual | In accordance with TX HB 300

Overview

Compliance with the Texas Medical Records Privacy Act (MRPA) – in accordance with TX HB 300, along with complying with the Security, Privacy, breach notifications, and other important measures of the Health Insurance Portability and Accountability Act - commonly known as HIPAA - requires organizations to gain a strong understanding of various provisions within MRPA, HIPAA and HITECH, along with becoming knowledgeable in regards to information security. This is best conducted by implementing a security awareness training program for all employees and other related third-party users for purposes of better understanding information security as a whole, and its applicability to MRPA and HIPAA compliance. The use of information technology is extremely widespread in today's society, ushering in unprecedented levels of cost-effectiveness and efficiency. Yet with great benefits also come great challenges, particularly when it comes to ensuring the confidentiality, integrity, and availability (CIA) of critical system components storing, processing and/or transferring sensitive and confidential information, such as Protected Health Information (PHI), Personally Identifiable Information (PII), and other important assets. It's imperative that all employees within [company name] and other in-scope users have a strong understanding of information security, such as being aware of dangers and challenges, while also being responsive in helping combat such threats and challenges with appropriate measures.

Security awareness is about effectively designing, developing, implementing, and maintaining an enterprise-wide program for which all employees can benefit from, one that implements the core components of **Awareness**, **Training**, and **Education**. Specifically, "Awareness" in that numerous measures are initiated and implemented for keeping all employees knowledgeable regarding threats, responses and solutions to security issues affecting an organization. "Training" in that material is researched, developed and subsequently utilized for educating employees on all aspects of security awareness. And lastly, "Education, in that adequate measures are undertaken for ensuring continuing education on security awareness is provided to all employees on a routine basis – whatever that may be – quarterly, annually, etc. It must be stressed that security awareness training is dynamic in nature, changing as needed to meet the growing threats facing today's organizations.

The subsequent documentation found herein is [company name]'s formal security awareness training program covering both general, best-of-breed practices for information security, along with specific measures relating to the safety and security of any PHI, PII, ePHI data - or any subset thereof - being stored, processed, and transmitted. Users are required to read the entire document annually, keep an electronic or hard-copy form readily available for referencing, along with signing and returning the acknowledgement form on the last page to authorized personnel at [company name]. You'll hear the following phrase repeated a number of times throughout this document - "if you see something, say something", which is the Department of Homeland Security's (DHS) motto for reporting suspicious activity – a motto that you should strive to adhere to at all times.

Goals

There are many challenges when it comes to MRPA and HIPAA security awareness training for today's organizations, such as time constraints, lack of interest by end-users, breaking from traditional practices, along with numerous other issues. As such, the [company name] security awareness training program seeks to successfully achieve the following goals:

- Provide a comprehensive, yet easy-to-understand and engaging training program.
- Offer in-depth educational resources regarding many of today's most critically important MRPA and HIPAA related security issues.
- Deliver a clear and concise messages as to the what security awareness is, why it's important, what it entails, and many other applicable issues.
- Enhance end-user skills, knowledge and overall awareness regarding information security.
- Encourage best practices for information security, while also fundamentally changing the way employees regard the need for security awareness provisions.
- Finally, making security awareness a true part of the organization's fabric, one that requires a commitment by ell employees for ultimately helping ensure the safety and security of [company name]'s critical system components.