Insert company logo here

HIPAA Security Awareness and Workforce Training Program Manual

[Company Name]

HIPAA Security Awareness and Workforce Training Program Manual

Insert Company Logo

HIPAA Security Awareness and Workforce Training Manual Program

Overview

Compliance 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 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 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 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 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 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 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.

As stated earlier, HIPAA security awareness training for [company name] encompasses measures relating to best-of-breed practices for information security, while also ensuring the safety and security of any PII, ePHI data - or any subset thereof - being stored, processed, and/or transmitted, along with other sensitive information. Moreover, the HIPAA security awareness training program is suitable for all employees, including senior management, I.T. personnel, along with all other end-users of [company name] system components. Topics covered within [company name]'s security awareness training program include the following:

- The Importance of Security Awareness Training
- Data Security Breaches
- What is Information Security?
- Roles and Responsibilities
- Information Security Solutions
- Defense-in-Depth
- Layered Security
- Cyber Security
- Cloud Computing
- HIPAA | Introduction
- HITECH | Introduction
- HIPAA Security Awareness Training Requirements
- HIPAA Security Rule
- HIPAA Security | 164.308 Administrative Safeguards
- HIPAA Security | 164.310 Physical Safeguards
- HIPAA Security | 164.312 Technical Safeguards
- HIPAA Security | Policies and Procedures
- HIPAA Notification of Breaches | As Amended by the Final Omnibus Ruling | January, 2013
- HIPAA Privacy Rule
- HIPAA Privacy | 164.500 - 164.534
- HIPAA Privacy | General Principles for Uses and Disclosures
- HIPAA Privacy | Permitted Uses and Disclosures
- HIPAA Privacy | Authorized Uses and Disclosures
- HIPAA Privacy | Individual Rights

- HIPAA Privacy | Administrative Requirements
- HIPAA Privacy | General Safeguards and Best Practices
- Covered Entities
- Business Associates
- Final Omnibus Ruling (January, 2013)
- Helpful HIPAA Resources
- FERPA
- FACTA
- Red Flags Rule
- PCI DSS
- GLBA
- Other Regulations
- Security Awareness Topics
- Account Security and Access Rights
- Malware
- Security Updates
- Clean Desk Policy
- Workstation Security
- Laptop Security
- Software Licensing and Usage
- Internal Threats
- Physical Security and Environmental Security
- Incident Response
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Protecting Information (Hard-Copy)
- Protecting Information (Electronic Format)
- Data Retention
- Identity Theft
- Online Security and Mobile Computing
- Shopping Online
- Securing Your Home Network
- Protecting your Children Online
- Security Tips for Travelling
- Other Important Security Awareness Considerations and Top Internet Scams
- If you see something, say something - Immediately
- Top 20 Security Considerations for I.T. Personnel
- Security Awareness Resources