TOPCERTIFIER
www.topcertifier.com

METODOLOGIA DEL SERVIZIO PER L'HIPAA

Portabilità dell'assicurazione sanitaria e legge sulla responsabilità

INTRODUZIONE ALL'HIPAA

L'HIPAA è una legge federale globale emanata per:

- Proteggere la privacy delle informazioni personali e sanitarie del paziente
- Fornire la sicurezza elettronica e fisica delle informazioni personali e sanitarie
- Standardizzare la codifica per semplificare la fatturazione e altre transazioni L'assicurazione sanitaria Il Portability and Accountability Act (HIPAA) riguarda la privacy, la sicurezza e la notifica di violazione Le regole proteggono la privacy e la sicurezza delle informazioni sanitarie e forniscono agli individui alcuni diritti alle loro informazioni sanitarie.
- La normativa sulla privacy che stabilisce gli standard nazionali per la protezione delle informazioni sanitarie (PHI) possono essere utilizzati e divulgati
- La Regola di Sicurezza, che specifica le misure di salvaguardia a tutela delle entità e delle loro attività i dipendenti devono attuare per proteggere la riservatezza, l'integrità e la disponibilità di informazioni sanitarie elettroniche protette (phi)
- La Breach Notificatio Rule, che richiede alle entità interessate di informare le persone interessate; Dipartimento della salute e dei servizi umani degli Stati Uniti (HHS); e in alcuni casi, i media di una violazionedi PHI non garantite.

CALCIO D'INIZIO

Il kickoff meeting è uno strumento essenziale per comunicare e pianificare l'esecuzione del progetto con un'ostruzione minima e per completare il progetto entro i tempi e i costi pianificati. ordine del giorno per la riunione iniziale è:

- Discussione del piano di progetto: include la discussione sulla responsabilità e sulla responsabilità di parti interessate. tappe fondamentali e risultati finali del progetto.

- Portata dei servizi

- Requisiti legali e normativi

CREAZIONE DEL CORE TEAM

- Nomina del CISO
- Nomina del Comitato per la Gestione della Sicurezza delle Informazioni.
- Nomina del responsabile della sicurezza HIPAA

FORMAZIONE SULLA CONSAPEVOLEZZA \ DELL'HIPAA

La formazione sulla consapevolezza HIPAA sarà condotta ai dipendenti della tua organizzazione. IL sessione di formazione è quella di aiutare i dipendenti ad acquisire conoscenze, comprendere i concetti di HIPAA, e allineare i processi e le pratiche verso il raggiungimento, la definizione, l'implementazione, mantenere e migliorare continuamente un ambiente di lavoro del sistema di gestione dei servizi. Una volta formato il personale, sarà possibile pensare, agire e contribuire al raggiungimento degli obiettivi obiettivi.

IMPLEMENTAZIONE IN FASE

FASE I - GAP ANALYSIS

Durante questa fase conduciamo un'analisi delle lacune per verificare quante delle vostre pratiche attuali sono in linea con i requisiti. Le tue pratiche attuali vengono verificate rispetto a questi quattro riferimenticriteri.

- Requisiti standard HIPAA
- Requisiti legali, regolamentari e statutari

I risultati di questa analisi sono presentati sotto forma di Gap Analysis Report. Questo rapporto funge da elenco di elementi di azione per il promemoria del progetto.

FASE II - ESECUZIONE DELLA VALUTAZIONE DEL RISCHIO HIPAA

Una procedura di gestione del rischio deve essere documentata e utilizzata come riferimento per gestire il rischi identificati in consultazione con tutti i responsabili delle funzioni dei proprietari dei processi. Utilizziamo la gestione del rischio tecniche come ISO 31000, ISO 27005,NIST,COBIT per identificare, analizzare, valutare, documentare, dare priorità, trattare, quantificare i rischi identificati. Questo passaggio crea un registro dei rischi. Rischio adatto i piani di trattamento sono individuati e attuati in base alla propensione al rischio dell'azienda, I risultati di tali azioni vengono calcolati, registrati, valutati e documentati. Audit periodici del rischio vengono effettuate al fine di garantire l'aderenza del sistema alla conformità.

FASE III - SVILUPPO DEL PIANO DI RISANAMENTO HIPAA

Dopo le valutazioni del rischio assistiamo nella progettazione del piano di riparazione HIPAA in base al rischio risultati della valutazione ciò avviene principalmente coordinandosi con i responsabili funzionali al fine di implementare in modo efficiente un piano di riparazione efficace e conforme a HIPAA in genere lo farà includere,

- Cosa è necessario fare per proteggere adeguatamente i dati privati dei pazienti
- Un calendario realistico per il completamento di queste attività
- Un elenco di quali membri del tuo team sono responsabili di quali attività
- Documentazione di seguito o completamento di queste attività

FASE IV - SVILUPPO DEL CONTRATTO DI ASSOCIAZIONE D'IMPRESA

Secondo HIPAA, persone o entità esterne alla tua forza lavoro che utilizzano o hanno accesso al tuo i dati PHI o phi del paziente nell'esecuzione del servizio per tuo conto sono considerati "soci in affari" assistiamo nello sviluppo e nella revisione degli accordi contrattuali dei soci in affari basati sul tipo di fornitore impegnato per un servizio specifico rispetto alla conformità HIPAA.

FASE] V - IMPOSTAZIONE DEL PROCESSO PER GLI INCIDENTI DI DATA BREACH

Forniamo assistenza nell'impostazione dei processi per identificare e gestire le violazioni dei dati PHI. (Es. HIPAA procedure di notifica delle violazioni) e anche assistere nello sviluppo di procedure sulla segnalazione degli incidenti meccanismo all'autorità di controllo interessata.

FASE VI - SUPPORTO DOCUMENTAZIONE HIPAA

Il piano di conformità HIPAA dovrebbe includere politiche e procedure che garantiscano la privacy di Informazioni sanitarie protette e sicurezza di tali informazioni. Le politiche di sicurezza e Le procedure riguardano il phi (PHI elettronico) e assistiamo nello sviluppo della privacy e della sicurezza HIPAA politiche e procedure per ciascuna funzione comprendendo il tipo di (phi) con cui si occupano rispetto all'HIPAA.

UFFICIALE DI SICUREZZA HIPAA INTERNO FORMAZIONE SULLA VERIFICA

La formazione per auditor interno (IA) HIPAA sarà fornita al responsabile della sicurezza HIPAA. Questa formazionefornirà a tale personale gli strumenti necessari per analizzare la necessità di IA, pianificare e programmare l'IA, preparare il controllo di auditelenchi, condurre una IA e documentare e riferire le proprie osservazioni al top management

AUDIT INTERNO HIPAA

I nostri esperti supervisioneranno la conduzione dell'audit interno da parte del responsabile della sicurezza HIPAA. Questo audit interno identificherà le lacune ancora esistenti nel sistema e ne dimostrerà il livello preparazione ad affrontare il controllo di conformità. Questo audit offre all'organizzazione la possibilità di farlo identificare e correggere tutte le non conformità prima di procedere al controllo di conformità. La parte superiore la direzione viene informata dei risultati dell'audit interno.

HIPAA - ANALISI DELLA CAUSA PRINCIPALE (RCA)E AZIONI CORRETTIVE

Tutte le non conformità identificate durante l'audit interno, gli audit del cliente o di terze parti o daRegistro dei rischi, valutazioni dei rischi dei fornitori, registri degli incidenti, registri di backup dei dati, violazione dei dati rapporti di notifica, è necessario elencare altre fonti. La RCA viene eseguita utilizzando tecniche come Metodi di brainstorming e Fish-Bone. La correzione ottimale e le azioni correttive sono implementate e l'efficacia di tali azioni è documentata e rivista tramite un HIPAA Rapporto sulle Azioni Correttive (CAR). I nostri esperti saranno presenti con il tuo team per guidarti attraverso il processo.

REVISIONE DELLA GESTIONE HIPAA RIUNIONE (MRM)

L'MRM è un'opportunità per tutte le parti interessate di incontrarsi a intervalli programmati per rivedere, discutere e pianificare azioni sui punti dell'ordine del giorno riportati di seguito.

- Registro dei rischi
- Deviazioni sugli aspetti di conformità
- Rapporti sulle attività post-consegna
- Piano d'azione per risolvere eventuali questioni aperte
- Opportunità di miglioramento, cambiamenti necessari nel sistema

VERIFICA DI CONFORMITÀ HIPAA

Quando i livelli di preparazione hanno raggiunto livelli adeguati, inizia il processo di Compliance inizia la certificazione. Un revisore nominato dell'Organismo di Vigilanza (OdC) verifica la preparazione tramite un audit esterno. Ciò implica che il revisore riveda le politiche, i processi, le POS, i fattori critici registri operativi e registri IA e MRM. Qualsiasi deviazione importante dalle aspettative della BC lo farà essere avvisato a questo punto per apportare le necessarie correzioni. Ciò riduce le possibilità di maggiorenon conformità durante l'audit di certificazione. TOPCertifier collaborerà con tutte le parti interessate e supervisionare il regolare completamento dell'audit.

CONTINUAZIONE DELLA CONFORMITÀ

TOPCertifier farà parte del percorso di conformità della tua organizzazione e ti assisterà regolarmente intervalli con la formazione necessaria, supporto e formazione del sistema, audit interni ed esterni e il rinnovo regolare della tua certificazione.