TOPCERTIFIER
www.topcertifier.com

MÉTHODOLOGIE DE SERVICE POUR LA HIPAA

Portabilité de l'assurance maladie et Loi sur la responsabilité

INTRODUCTION À LA HIPAA

HIPAA est une loi fédérale complète promulguée pour :

- Protéger la confidentialité des informations personnelles et de santé d'un patient

- Assurer la sécurité électronique et physique des informations personnelles et de santé

- Standardiser le codage pour simplifier la facturation et d'autres transactions. L'Assurance Maladie La loi sur la portabilité et la responsabilité (HIPAA) implique des notifications en matière de confidentialité, de sécurité et de violation. Les règles protègent la confidentialité et la sécurité des informations sur la santé et offrent aux individus certains droits sur leurs informations de santé.

- La règle de confidentialité qui définit les normes nationales relatives aux informations de santé protégées (PHI) peut être utilisé et divulgué

- La règle de sécurité, qui spécifie les garanties qui couvraient les entités et leurs activités les associés doivent mettre en œuvre pour protéger la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé (phi)

- La règle de notification des violations, qui oblige les entités couvertes à notifier les personnes concernées ; Département américain de la Santé et des Services sociaux (HHS) ; et dans certains cas, les médias d'une violation

DÉMARRER

La réunion de lancement est un outil essentiel pour communiquer et planifier l'exécution du projet avec un minimum d'obstruction et pour terminer le projet dans les délais et les coûts prévus. Ordre du jour pour la réunion de lancement est :

- Discussion sur le plan de projet : cela inclut une discussion sur la responsabilisation et la responsabilité des parties prenantes. les jalons et les livrables du projet

- Portée des services

- Exigences légales et réglementaires

CRÉATION DE L'ÉQUIPE DE BASE

- RSSI de Penunjukan
- Penunjukan Komite Manajemen Keamanan Informasi
- Pétugas Penunjukan Keamanan HIPAA

TOPCERTIFIER
www.topcertifier.com

FORMATION DE SENSIBILISATION HIPAA

Une formation de sensibilisation à la HIPAA sera dispensée aux employés de votre organisation. La session de formation vise à aider les employés à acquérir des connaissances, à comprendre les concepts de la HIPAA, et aligner les processus et les pratiques pour atteindre et établir, mettre en œuvre, maintenir et améliorer continuellement un environnement de travail lié au système de gestion des services. Lorsque le personnel a été formé, il peut penser, agir et contribuer à la réalisation des objectifs. objectifs

MISE EN ŒUVRE PAR PHASES

PHASE I - ANALYSE DES ÉCARTS

Au cours de cette phase, nous effectuons une analyse des écarts pour vérifier dans quelle mesure vos pratiques actuelles sont conforme aux exigences. Vos pratiques actuelles sont vérifiées par rapport à ces quatre références critères.

- Exigences de la norme HIPAA

- Exigences légales, réglementaires et statutaires Les résultats de cette analyse sont présentés sous la forme d'un rapport d'analyse des écarts. Ce rapport fait office de liste d'éléments d'action pour le rappel du projet.

PHASE II - RÉALISATION D'UNE ÉVALUATION DES RISQUES HIPAA

Une procédure de gestion des risques doit être documentée et utilisée comme référence pour gérer les risques identifiés en consultation avec tous les chefs de fonction des propriétaires de processus. Nous utilisons la gestion des risques des techniques comme ISO 31000, ISO 27005, NIST, COBIT pour identifier, analyser, évaluer, documenter, prioriser, traiter quantifier les risques identifiés. Cette étape crée un registre des risques. Risque approprié des plans de traitement sont identifiés et mis en œuvre en fonction de l'appétit pour le risque de l'entreprise, Les résultats de ces actions sont calculés, enregistrés, évalués et documentés. Audits périodiques des risques sont réalisées afin de garantir le respect du système à la conformité.

PHASE III – DÉVELOPPEMENT D'UN PLAN DE REMÉDIATION HIPAA

Après les évaluations des risques, nous aidons à la conception d'un plan de remédiation HIPAA basé sur le risque. résultats de l'évaluation, cela se fait principalement en coordination avec les responsables fonctionnels afin de mettre en œuvre de manière efficace un plan de remédiation efficace et conforme à la HIPAA. inclure,

- Que faut-il faire pour sécuriser correctement les données privées de vos patients ?
- Un calendrier réaliste pour que ces tâches soient accomplies
- Une liste des membres de votre équipe qui sont responsables de quelles tâches
- Documentation du suivi ou de l'achèvement de ces tâches

PHASE IV - DÉVELOPPEMENT D'UN CONTRAT D'ASSOCIATION D'ENTREPRISE

En vertu de la HIPAA, les personnes ou entités extérieures à votre personnel qui utilisent ou ont accès à votre les PHI ou phi du patient effectuant un service en votre nom sont appelés « Associés commerciaux » nous aidons à développer et à réviser les accords contractuels des associés commerciaux sur la base de le type de fournisseur qui est engagé pour un service spécifique en ce qui concerne HIPAA Conformités.

PHASE V - MISE EN PLACE DU PROCESSUS POUR LES INCIDENTS DE VIOLATION DE DONNÉES

Nous aidons à mettre en place les processus permettant d'identifier et de gérer les violations de données PHI. (Par exemple. HIPAA procédures de notification des violations) et aident également à élaborer des procédures de rapport d'incident mécanisme à l'autorité de contrôle concernée.

PHASE VI - SOUTIEN À LA DOCUMENTATION HIPAA

Le plan de conformité HIPAA doit inclure des politiques et des procédures garantissant la confidentialité des Informations de santé protégées et sécurité de ces informations. Les politiques de sécurité et Les procédures traitent des phi (PHI électroniques). Nous aidons au développement de la confidentialité et de la sécurité HIPAA. politiques et procédures pour chaque fonction en comprenant le type de (phi) avec lequel elles gèrent respect de la HIPAA.

AGENT DE SÉCURITÉ HIPAA INTERNE FORMATION À L'AUDIT

Une formation d'auditeur interne (IA) HIPAA sera dispensée au responsable de la sécurité HIPAA. Cette formation équipera ce personnel pour analyser le besoin d'IA, planifier et planifier l'IA, préparer le contrôle d'audit listes, et mener une IA et documenter et rapporter leurs observations à la haute direction

AUDIT INTERNE HIPAA

Nos experts superviseront la conduite de l'audit interne par votre responsable de la sécurité HIPAA. Cet audit interne identifiera les lacunes encore existantes dans le système et démontrera le niveau de préparation à faire face à l'audit de conformité. Cet audit donne à l'organisation une chance de identifier et rectifier toutes les non-conformités avant de procéder à l'audit de conformité. Le sommet la direction est informée des conclusions de l'audit interne.

HIPAA - ANALYSE AKAR PENYEBAB (RCA) DAN TINDAKAN KOREKTIF

Toutes les non-conformités identifiées lors de l'audit interne, des audits clients ou tiers, ou du Registre des risques, évaluations des risques des fournisseurs, journaux d'incidents, journaux de sauvegarde des données, violation de données rapports de notification, d'autres sources doivent être répertoriées. RCA est réalisé en utilisant des techniques telles que Méthodes de brainstorming et Fish-Bone. La correction optimale et les actions correctives sont mises en œuvre et l'efficacité de ces actions est documentée et examinée via un HIPAA Rapport d'action corrective (CAR). Nos experts seront présents avec votre équipe pour vous guider tout au long du processus.

EXAMEN DE LA GESTION HIPAA RÉUNION (MRM)

Le MRM est l'occasion pour toutes les parties prenantes de se réunir à intervalles réguliers pour examiner, discuter et planifier des actions sur les points ci-dessous de l'ordre du jour.

- Registre des risques
- Écarts sur les aspects de conformité
- Rapports d'activités après livraison
- Plan d'action pour résoudre les éléments non soldés
- Possibilités d'amélioration, changements nécessaires dans le système

AUDIT DE CONFORMITÉ HIPAA

Lorsque les niveaux de préparation ont atteint des niveaux adéquats, le processus de conformité la certification commence. Un auditeur désigné du Compliance Body (CB) vérifie l'état de préparation via un audit externe. Cela implique que l'auditeur examine les politiques, les processus, les SOP, les dossiers opérationnels et les dossiers IA et MRM. Tout écart majeur par rapport aux attentes de la BC être notifié à ce stade pour apporter les corrections nécessaires. Cela réduit les risques de blessures majeures non-conformités lors de l'audit de certification. TOPCertifier assurera la liaison avec toutes les parties prenantes et superviser la bonne réalisation de l'audit.

POURSUITE DE LA CONFORMITÉ

TOPCertifier fera partie du parcours de conformité de votre organisation et vous assistera régulièrement intervalles avec les formations nécessaires, le support système et les pupations, les audits internes et externes et le renouvellement régulier de votre certification.