TOPCERTIFIER
www.topcertifier.com

サービス方法論
のために HIPAA

健康保険のポータビリティ
および責任法

TOPCERTIFIER
www.topcertifier.com

はじめに HIPAA

HIPAA は、次の目的で制定された包括的な連邦法です。

- 患者の個人情報と健康情報のプライバシーを保護します
- 個人情報と健康情報の電子的および物理的セキュリティを提供する
- コーディングを標準化して請求やその他のトランザクションを簡素化する 健康保険移植性と責任に関する法律 (HIPAA) には、プライバシー、セキュリティ、侵害通知が含まれます 規則は健康情報のプライバシーとセキュリティを保護し、個人に以下の情報を提供します。自分の健康情報に対する一定の権利
- 医療情報を保護する場合の国家基準を設定するプライバシー規則 (PHI) 使用および開示される場合があります
- セキュリティ ルール。エンティティとそのビジネスを対象とする保護措置を指定します。従業員は、機密性、完全性、および可用性を保護するために実装する必要があります。電子保護医療情報 (phi)
- 侵害通知ルール。対象となる組織が影響を受ける個人に通知することを義務付けます。米国保健福祉省 (HHS);場合によっては、侵害のメディア
安全でない PHI の

キックオフ

キックオフ ミーティングは、プロジェクトの実行に関するコミュニケーションと計画を立てるための重要なツールです 障害を最小限に抑え、計画された時間とコスト内でプロジェクトを完了します。議題 キックオフミーティングは :

- プロジェクト計画のディスカッション: これには、責任と責任に関するディスカッションが含まれます。 関係者。プロジェクトのマイルストーンと成果物

- サービスの範囲

- 法的および規制上の要件

コアチームの創設

- CISOの任命
- 情報セキュリティ管理委員会を設置
- HIPAA セキュリティ担当者の任命

TOPCERTIFIER
www.topcertifier.com

HIPAA 認識トレーニング

HIPAA 意識向上トレーニングが組織の従業員に対して実施されます。の トレーニング セッションは、従業員が知識を獲得し、HIPAA の概念を理解し、達成および確立、実装に向けてプロセスと実践を調整し、 サービス管理システムの作業環境を維持し、継続的に改善します。 スタッフがトレーニングを受けると、考えて行動し、目標の達成に貢献できるようになります。 目標。

段階的な実装

フェーズ I - ギャップ分析

このフェーズでは、ギャップ分析を実施して、現在の実践がどの程度適切であるかを確認します。要件に沿って。あなたの現在の実践は、次の 4 つの基準に照らして検証されます基準。

- HIPAA 標準要件
- 法律、規制、法定の要件

この分析の結果は、ギャップ分析レポートの形式で表示されます。 この報告書プロジェクトを思い出させるためのアクション アイテムのリストとして機能します。

フェーズ II - HIPAA リスク評価の実施

リスク管理手順は文書化され、リスク管理の参考として使用されます。すべてのプロセス所有者の部門責任者と協議してリスクを特定します。私たちはリスク管理を行っています ISO 31000、ISO 27005、NIST、COBIT などの特定、分析、評価、文書化、特定されたリスクを定量化し、優先順位を付けて対処します。このステップでは、リスク登録を作成します。適切なリスク 治療計画は企業のリスクアペタイトに基づいて特定され、実行されます。 このようなアクションの結果は計算され、記録され、評価され、文書化されます。定期的なリスク監査 システムがコンプライアンスを遵守していることを確認するために実行されています。

フェーズ III – HIPAA 修復計画の策定

リスク評価後、リスクに基づいた HIPAA 改善計画の設計を支援します。評価結果を評価するために、これは主に部門責任者と調整することによって行われます。 通常、HIPAA に準拠した効果的な改善計画を効率的な方法で実装します。 含む、

- 患者の個人データを適切に保護するには何が必要か
- これらのタスクを完了するための現実的な時間枠
- チームのどのメンバーがどのタスクを担当するかのリスト
- これらのタスクのフォロースルーまたは完了の文書化

フェーズ IV – ビジネスアソシエイト契約契約の開発

HIPAA に基づいて、あなたの従業員以外の個人または団体があなたのデータを使用またはアクセスすることを指します。 患者の PHI またはあなたに代わってサービスを実行する PH は、「業務提携者」と言われます。私たちは、以下に基づいて取引先契約書の作成とレビューを支援します。HIPAA に関して特定のサービスに従事しているベンダーの種類
コンプライアンス。

フェーズ V – データ侵害インシデントのプロセスの設定

当社は、PHI データ侵害を特定して対処するためのプロセスの設定を支援します。(例:HIPAA 違反通知手順）、インシデント報告に関する手順の作成も支援します。当該メカニズムを関係監督当局に報告する。

フェーズ VI – HIPAA 文書サポート

HIPAA コンプライアンス計画には、プライバシーを確保するポリシーと手順を含める必要があります。保護された健康情報とそのような情報のセキュリティ。セキュリティポリシーとphi (電子 PHI) に関する手順は、HIPAA のプライバシーとセキュリティの開発を支援します。処理する (ファイ) の種類を理解することで、各機能のポリシーと手順を理解する
HIPAA に敬意を表します。

HIPAA 社内セキュリティ担当者監査トレーニング

HIPAA 内部監査人 (IA) トレーニングは、HIPAA セキュリティ担当者に提供されます。この研修はIAの必要性を分析し、IAを計画およびスケジュールし、監査チェックを準備できる人材を養成します。リストを作成し、IA を実施し、観察結果を文書化して経営トップに報告する

TOPCERTIFIER
www.topcertifier.com

HIPAA 内部監査

当社の専門家は、HIPAA セキュリティ担当者による内部監査の実施を監督します。この内部監査は、システム内に依然として存在するギャップを特定し、システムのレベルを実証します。 コンプライアンス監査に直面する準備。 この監査は組織に次の機会を与えます。コンプライアンス監査に進む前に、すべての不適合を特定して修正します。頂上 経営陣には内部監査の結果が通知されます。

HIPAA - 根本原因分析（RCA）および是正措置

内部監査、クライアントまたは第三者の監査中に特定されたすべての不適合、またはリスク登録、ベンダーリスク評価、インシデントログ、データバックアップログ、データ侵害 通知レポートの場合、他のソースをリストする必要があります。 RCA は次のような手法を使用して実行されます。ブレーンストーミングとフィッシュボーン手法。最適な修正と是正措置は次のとおりです。実施され、そのような措置の有効性が文書化され、HIPAA を通じてレビューされます。 是正措置報告書 (CAR)。

当社の専門家が貴社のチームに同行し、プロセスをガイドします。

HIPAA 管理レビューミーティング（MRM）

MRM は、すべての関係者が予定された間隔で集まり、レビューを行う機会です。以下の議題について話し合い、行動を計画する.

- リスクレジスター
- コンプライアンス面での逸脱
- 納品後の活動報告
- 未解決の項目を解決するための行動計画
- 改善の機会、システムに必要な変更

TOPCERTIFIER
www.topcertifier.com

HIPAA コンプライアンス監査

準備レベルが適切なレベルに達すると、コンプライアンスのプロセスが開始されます。認証が始まります。コンプライアンス機関 (CB) の任命された監査人が準備状況を検証します。外部監査を通じて。これには、監査人がポリシー、プロセス、SOP、重要な事項をレビューすることが含まれます。 運用記録、IA および MRM 記録。 CB の期待からの大きな逸脱は、この時点で必要な修正を行うよう通知されます。これにより重大事故の可能性が減ります認証監査中の不適合。 TOPCertifier はすべての関係者と連携します。監査がスムーズに完了するよう監督します。

コンプライアンスの継続

TOPCertifier は、組織のコンプライアンスへの取り組みの一部となり、定期的なコンプライアンスの遵守を支援します。 必要なトレーニング、システムサポートと蛹化、内部および外部監査の間隔 定期的に認定を更新します。