TOPCERTIFIER
www.topcertifier.com

SERVICEMETHODOLOGIE VOOR HIPAA

Health Insurance Portability and Accountability Act

INLEIDING TOT HIPAA

HIPAA is een alomvattende federale wet die is uitgevaardigd om:

- Bescherm de privacy van de persoonlijke en gezondheidsinformatie van een patiënt
- Zorg voor elektronische en fysieke beveiliging van persoonlijke en gezondheidsinformatie
- Standaardiseer de codering om facturering en andere transacties te vereenvoudigen. De zorgverzekering Portability and Accountability Act (HIPAA) omvat privacy, beveiliging en melding van inbreuken Regels beschermen de privacy en veiligheid van gezondheidsinformatie en voorzien individuen ervan bepaalde rechten op hun gezondheidsinformatie
- De Privacyregel die nationale normen vaststelt voor beschermde gezondheidsinformatie (PHI) mag worden gebruikt en openbaar gemaakt
- De Security Rule, die waarborgen specificeert die betrekking hebben op entiteiten en hun activiteiten medewerkers moeten implementeren om de vertrouwelijkheid, integriteit en beschikbaarheid van te beschermen elektronisch beschermde gezondheidsinformatie (phi)
- De Breach Notificatio Rule, die vereist dat gedekte entiteiten getroffen personen op de hoogte stellen; U.S. Ministerie van Volksgezondheid en Human Services (HHS); en in sommige gevallen de media op de hoogte van een inbreukvan onbeveiligde PHI

AFTRAP

De kickoff meeting is een essentieel instrument om te communiceren en plannen te maken voor de uitvoering van het project met minimale belemmering en om het project binnen de geplande tijd en kosten te voltooien. Agenda voor de kick-off bijeenkomst is:

- Bespreking van het projectplan: Dit omvat discussie over aansprakelijkheid en verantwoordelijkheid van
  belanghebbenden. mijlpalen en resultaten in het project

- Omvang van de diensten

- Wettelijke en regelgevende vereisten

CREATIE VAN EEN KERNTEAM

- Benoeming van CISO
- Benoeming van het Informatiebeveiligingsbeheerscomité
- Benoeming van een HIPAA-beveiligingsfunctionaris

HIPAA-BEWUSTWORDINGSTRAINING

Er wordt een HIPAA-bewustzijnstraining gegeven aan de medewerkers van uw organisatie. De De trainingssessie is bedoeld om werknemers te helpen kennis op te doen, de concepten van HIPAA te begrijpen, en processen en praktijken op één lijn brengen met het oog op het bereiken en vaststellen, implementeren, het onderhouden en voortdurend verbeteren van de werkomgeving van een servicemanagementsysteem. Wanneer medewerkers zijn opgeleid, kunnen zij denken en handelen en bijdragen aan het realiseren van de doelstellingen doelen.

FASEGEWIJZE IMPLEMENTATIE

FASE I - GAP-ANALYSE

Tijdens deze fase voeren we een gap-analyse uit om te controleren hoeveel van uw huidige praktijken zijn in lijn met de eisen. Uw huidige praktijken worden geverifieerd aan de hand van deze vier referenties criteria.

- HIPAA-standaardvereisten
- Wettelijke, regelgevende en wettelijke vereisten De resultaten van deze analyse worden gepresenteerd in de vorm van een Gap Analysis Report. Dit rapport fungeert als de lijst met actiepunten ter herinnering aan het project

FASE II - UITVOEREN VAN HIPAA-RISICOBEOORDELING

Er moet een risicobeheerprocedure worden gedocumenteerd en gebruikt als referentie voor het beheer van de risicobeheerprocedure geïdentificeerde risico's in overleg met alle functiehoofden van proceseigenaren. Wij maken gebruik van risicomanagement technieken zoals ISO 31000, ISO 27005,NIST,COBIT voor het identificeren, analyseren, evalueren, documenteren, prioriteren, behandelen, de geïdentificeerde risico's kwantificeren. Met deze stap wordt een risicoregister gemaakt. Geschikt risico behandelplannen worden geïdentificeerd en geïmplementeerd op basis van de risicobereidheid van het bedrijf, De uitkomsten van dergelijke acties worden berekend, vastgelegd, geëvalueerd en gedocumenteerd. Periodieke risicoaudits worden uitgevoerd om ervoor te zorgen dat het systeem aan de voorschriften voldoet.

FASE III - ONTWIKKELING VAN HIPAA-SANERINGSPLAN

Na risicobeoordelingen helpen we bij het ontwerpen van een HIPAA-herstelplan op basis van het risico beoordelingsresultaten gebeurt dit vooral door afstemming met functionele hoofden het op efficiënte wijze implementeren van een effectief, HIPAA-conform herstelplan zal dat doorgaans ook doen erbij betrekken,

- Wat er moet gebeuren om uw privé-patiëntgegevens goed te beveiligen
- Een realistisch tijdsbestek waarin deze taken moeten worden voltooid
- Een lijst met welke leden van uw team verantwoordelijk zijn voor welke taken
- Documentatie van de opvolging of voltooiing van deze taken

FASE IV – ONTWIKKELING VAN CONTRACTOVEREENKOMST VOOR ZAKELIJKE PARTNERS

Onder HIPAA kunnen personen of entiteiten buiten uw personeelsbestand die gebruik maken van of toegang hebben tot uw De PHI of phi van de patiënt bij het uitvoeren van diensten namens u worden 'Zakenpartners' genoemd wij helpen bij het ontwikkelen en beoordelen van contractovereenkomsten met zakenpartners op basis van het type leverancier dat wordt ingeschakeld voor een specifieke dienst met betrekking tot HIPAA Nalevingen.

FASE V – PROCES OPZETTEN VOOR INCIDENTEN VAN GEGEVENSBREUK

Wij helpen bij het opzetten van de processen om PHI-gegevenslekken te identificeren en af te handelen. (Bijv. HIPAA meldingsprocedures voor inbreuken) en helpen ook bij het ontwikkelen van procedures voor het melden van incidenten mechanisme aan de betrokken toezichthoudende autoriteit.

FASE VI – ONDERSTEUNING VAN HIPAA-DOCUMENTATIE

Het HIPAA-nalevingsplan moet beleid en procedures omvatten die de privacy van Beschermde gezondheidsinformatie en de beveiliging van dergelijke informatie. Het veiligheidsbeleid en Procedures hebben betrekking op phi (elektronische PHI). Wij helpen bij het ontwikkelen van HIPAA-privacy en -beveiliging beleid en procedures voor elke functie door inzicht te krijgen in het type (phi) waarmee ze omgaan respect voor HIPAA.

HIPAA-BEVEILIGINGSOFFICIER INTERN AUDIT-TRAINING

Er wordt een HIPAA Internal Auditor (IA)-training gegeven aan de HIPAA-beveiligingsfunctionaris. Deze opleidingzal dergelijk personeel uitrusten om de behoefte aan IA te analyseren, IA te plannen en in te plannen, en auditcontroles voor te bereidenen het uitvoeren van een evaluatie, en het documenteren en rapporteren van hun observaties aan het topmanagement

HIPAA INTERNE AUDIT

Onze experts houden toezicht op de uitvoering van de interne audit door uw HIPAA-beveiligings functionaris. Deze interne audit zal nog bestaande hiaten in het systeem identificeren en het niveau ervan aantonen voorbereiding op de nalevingsaudit. Deze audit geeft de organisatie daartoe de kans alle niet-nalevingen identificeren en corrigeren voordat u doorgaat met de nalevingsaudit. De bovenkant Het management wordt op de hoogte gesteld van de bevindingen van de interne audit.

HIPAA - OORZAAKANALYSE (RCA) EN CORRIGERENDE ACTIES

Alle non-conformiteiten die zijn vastgesteld tijdens de interne audit, audits van klanten of derden, of vanRisicoregister, risicobeoordelingen van leveranciers, incidentlogboeken, logboeken voor gegevensback-ups, gegevensinbreuk kennisgevingsrapporten moeten andere bronnen worden vermeld. RCA wordt uitgevoerd met behulp van technieken zoals Brainstormen en visgraatmethoden. De optimale correctie en corrigerende acties zijn geïmplementeerd en de effectiviteit van dergelijke acties wordt gedocumenteerd en beoordeeld via een HIPAA Rapport met corrigerende maatregelen (CAR).
Onze experts zijn samen met uw team aanwezig om u door het proces te begeleiden.

HIPAA-MANAGEMENTREVIEW VERGADERING (MRM)

Het MRM is een gelegenheid voor alle belanghebbenden om met geplande tussenpozen bijeen te komen om de bespreek en plan acties op de onderstaande agendapunten.

- Risicoregister
- Afwijkingen op compliance-aspecten
- Activiteitenrapporten na de bevalling
- Actieplan om eventuele openstaande posten op te lossen
- Kansen voor verbetering, veranderingen nodig in het systeem

HIPAA-NALEVING-AUDIT

Wanneer de niveaus van paraatheid een adequaat niveau hebben bereikt, begint het proces voor compliance certificering begint. Een aangewezen auditor van het Toezichtsorgaan (CI) verifieert de paraatheid via een externe audit. Dit houdt in dat de auditor het beleid, de processen en de SOP's beoordeelt die cruciaal zijn operationele gegevens en IA- en MRM-gegevens. Bij grote afwijkingen van de verwachting van de CI zal dat wel het geval zijn op dit punt op de hoogte worden gesteld voor het doorvoeren van de noodzakelijke correcties. Dit verkleint de kans op een majornon-conformiteiten tijdens de certificatieaudit. TOPCertifier onderhoudt contacten met alle belanghebbenden en toezicht houden op de voltooiing van de audit.

VOORTZETTING VAN NALEVING

TOPCertifier zal deel uitmaken van het compliance-traject van uw organisatie en u regelmatig assisteren intervallen met noodzakelijke trainingen, systeemondersteuning en pupaties, interne en externe audits en regelmatige verlenging van uw certificering.