



METODOLOGIA DE ATENDIMENTO PARA HIPAA

**Portabilidade de Seguro Saúde
e Lei de Responsabilidade**

INTRODUÇÃO À HIPAA

HIPAA é uma lei federal abrangente promulgada para:

- Proteger a privacidade das informações pessoais e de saúde de um paciente
- Fornecer segurança eletrônica e física de informações pessoais e de saúde
- Padronize a codificação para simplificar o faturamento e outras transações O Seguro de Saúde A Lei de Portabilidade e Responsabilidade (HIPAA) envolve privacidade, segurança e notificação de violação As regras protegem a privacidade e a segurança das informações de saúde e fornecem aos indivíduos certos direitos às suas informações de saúde.
- A Regra de Privacidade que estabelece padrões nacionais para informações de saúde protegidas (PHI) podem ser usados e divulgados
- A Regra de Segurança, que especifica salvaguardas que abrangem entidades e seus negócios associados devem implementar para proteger a confidencialidade, integridade e disponibilidade de informações eletrônicas de saúde protegidas (phi)
- A Regra de Notificação de Violação, que exige que as entidades cobertas notifiquem os indivíduos afetados; Departamento de Saúde e Serviços Humanos dos EUA (HHS); e, em alguns casos, a mídia de uma violação de PHI não seguras.

COMEÇO

A reunião de kickoff é uma ferramenta essencial para comunicar e planejar a execução do projeto com obstrução mínima e concluir o projeto dentro do tempo e custo planejados. Agenda para a reunião inicial é:

- Discussão do plano do projeto: Inclui discussão sobre prestação de contas e responsabilidade de partes interessadas. marcos e entregas do projeto.
- Escopo dos serviços
- Requisitos legais e regulamentares

CRIAÇÃO DA EQUIPE NÚCLEO

- Nomeação do CISO
- Nomeação do Comitê de Gestão de Segurança da Informação.
- Nomeação do oficial de segurança HIPAA

TREINAMENTO DE CONSCIENTIZAÇÃO HIPAA

O treinamento de conscientização HIPAA será realizado para os funcionários da sua organização. O sessão de treinamento é ajudar os funcionários a adquirir conhecimento, compreender os conceitos da HIPAA, e alinhar processos e práticas para alcançar e estabelecer, implementar, manter e melhorar continuamente um ambiente de trabalho do sistema de gerenciamento de serviços. Quando os funcionários são treinados, eles podem pensar e agir e contribuir para alcançar os objetivos metas.

IMPLEMENTAÇÃO SÁBIA DE FASE

FASE I - ANÁLISE DE GAP

Durante esta fase, realizamos uma análise de lacunas para verificar o quanto de suas práticas atuais são de acordo com os requisitos. Suas práticas atuais são verificadas em relação a estas quatro referênciascritérios.

- Requisitos padrão HIPAA
- Requisitos legais, regulamentares e estatutários

Os resultados desta análise são apresentados na forma de um Relatório de Análise de Gap. Este relatório atua como a lista de itens de ação para o lembrete do projeto.

FASE II - REALIZANDO AVALIAÇÃO DE RISCO HIPAA

Um procedimento de Gestão de Risco deve ser documentado e usado como referência para gerenciar o identifiquei os riscos em consulta com todos os chefes de função dos proprietários de processos. Usamos gerenciamento de risco técnicas como ISO 31000, ISO 27005, NIST, COBIT para identificar, analisar, avaliar, documentar, priorizar, tratar, quantificar os riscos identificados. Esta etapa cria um Registro de Riscos. Risco Adequado os planos de tratamento são identificados e implementados com base no apetite ao risco da empresa, Os resultados de tais ações são calculados, registrados, avaliados e documentados. Auditorias periódicas de risco estão sendo realizados para garantir a aderência do sistema à conformidade.

FASE III - DESENVOLVIMENTO DO PLANO DE REMEDIAÇÃO DA HIPAA

Após avaliações de risco, auxiliamos na elaboração do plano de remediação da HIPAA com base no risco resultados da avaliação, isso é feito principalmente através da coordenação com chefes funcionais, a fim de implementar de maneira eficiente um plano de remediação eficaz e compatível com HIPAA normalmente incluir,

- O que precisa ser feito para proteger adequadamente os dados privados dos seus pacientes
- Um prazo realista para que essas tarefas sejam concluídas
- Uma lista de quais membros da sua equipe são responsáveis por quais tarefas
- Documentação de acompanhamento ou conclusão dessas tarefas

FASE IV - DESENVOLVIMENTO DO CONTRATO DE ASSOCIADO COMERCIAL

De acordo com a HIPAA, pessoas ou entidades fora da sua força de trabalho que usam ou têm acesso ao seu PHI ou phi do paciente na prestação de serviços em seu nome são consideradas "Parceiros Comerciais" auxiliamos no desenvolvimento e revisão de acordos contratuais de parceiros de negócios com base em o tipo de fornecedor que está sendo contratado para serviços específicos em relação à HIPAA Conformidades.

FASE V - CONFIGURAÇÃO DO PROCESSO PARA INCIDENTES DE VIOLAÇÃO DE DADOS

Ajudamos na configuração de processos para identificar e lidar com violações de dados PHI. (Ex. HIPAA procedimentos de notificação de violação) e também auxiliar no desenvolvimento de procedimentos de relatório de incidentes mecanismo à autoridade de supervisão em causa.

FASE VI - SUPORTE À DOCUMENTAÇÃO HIPAA

O Plano de Conformidade HIPAA deve incluir Políticas e Procedimentos que garantam a Privacidade de Informações de saúde protegidas e a segurança de tais informações. As Políticas de Segurança e Os procedimentos tratam de phi (PHI eletrônico), auxiliamos no desenvolvimento de privacidade e segurança HIPAA políticas e procedimentos para cada função, entendendo o tipo de (phi) com o qual elas lidam respeito à HIPAA.

OFICIAL DE SEGURANÇA HIPAA INTERNO TREINAMENTO DE AUDITORIA

O treinamento de auditor interno (IA) da HIPAA será fornecido ao oficial de segurança da HIPAA. Este treinamento equipará esse pessoal para analisar a necessidade de IA, planejar e programar IA, preparar verificação de auditorialistas, e conduzir uma IA e documentar e relatar suas observações à alta administração



AUDITORIA INTERNA HIPAA

Nossos especialistas supervisionarão a condução da auditoria interna pelo seu oficial de segurança HIPAA. Esta auditoria interna identificará lacunas ainda existentes no sistema e demonstrará o nível de preparação para enfrentar a auditoria de conformidade. Esta auditoria dá à organização a oportunidade de identificar e retificar todas as não conformidades antes de prosseguir para a auditoria de conformidade. O topo a administração é notificada das conclusões da auditoria interna.

HIPAA - ANÁLISE DE CAUSA RAIZ (RCA) E AÇÕES CORRETIVAS


Todas as não conformidades identificadas durante a auditoria interna, auditorias de clientes ou de terceiros, ou de Registro de riscos, avaliações de risco de fornecedores, registros de incidentes, registros de backup de dados, violação de dados relatórios de notificação, outras fontes devem ser listadas. RCA é realizada usando técnicas como Métodos Brainstorming e Fish-Bone. A correção ideal e as ações corretivas são implementado e a eficácia de tais ações é documentada e revisada por meio de um HIPAA Relatório de Ações Corretivas (CAR). Nossos especialistas estarão presentes com sua equipe para orientar durante o processo.

REVISÃO DE GESTÃO DA HIPAA REUNIÃO (MRM)

O MRM é uma oportunidade para todas as partes interessadas se reunirem em intervalos programados para analisar, discutir e planejar ações sobre os pontos da agenda abaixo.


- Registro de riscos
- Desvios em aspectos de compliance
- Relatórios de atividades pós-entrega
- Plano de ação para resolver quaisquer itens em aberto
- Oportunidades de melhoria, mudanças necessárias no sistema

AUDITORIA DE CONFORMIDADE HIPAA



Quando os níveis de preparação atingirem níveis adequados, o processo de Compliance começa a certificação. Um auditor nomeado do Órgão de Conformidade (OC) verifica a preparação através de uma auditoria externa. Isto envolve a revisão pelo auditor das políticas, processos, POPs, registros operacionais e registros IA e MRM. Quaisquer desvios importantes das expectativas do BC serão ser notificado neste momento para trazer as correções necessárias. Isso reduz as chances de grandes não conformidades durante a auditoria de certificação. TOPCertifier entrará em contato com todas as partes interessadas e supervisionar a conclusão tranquila da auditoria.

CONTINUAÇÃO DA CONFORMIDADE



TOPCertifier fará parte da jornada de conformidade da sua organização e ajudará você regularmente intervalos com treinamentos necessários, suporte de sistema e pupações, auditorias internas e externas e renovação regular de sua certificação.