



MUST
UNIVERSITY
FLORIDA - USA

HIPAA

Health Insurance Portability
and Accountability Act

**QUESTÕES RELACIONADAS A HEALTH
INSURANCE PORTABILITY AND
ACCOUNTABILITY ACT (HIPAA)**





QUESTÕES RELACIONADAS A HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Conteúdo organizado por **Millena Prata Jammal** em 2022 do livro **Ethical and Legal Issues in Healthcare**, publicado em 2018 por David Lemberg, pela editora **Cognella Academic Publishing**.

Objetivos de Aprendizagem

- Compreender a legislação no contexto da ética em saúde e as questões éticas relacionadas a *HIPAA*;
- Conhecer os *principais componentes da HIPAA*.

Introdução

Todas as pessoas têm direito à confidencialidade, exceto se concederem permissão para divulgação. A privacidade é reconhecida como um direito humano básico nos Estados Unidos. As leis de privacidade e segurança estão evoluindo continuamente para se ajustar a novos desafios, novas tecnologias e novas ameaças na era digital.

Em 1948, a Assembleia Geral das Nações Unidas (*United Nations General Assembly*) adotou a Declaração Universal dos Direitos Humanos e consagrou a privacidade como um direito humano fundamental, onde toda pessoa tem direito à proteção da lei contra interferências ou ataques.

Hoje, definimos privacidade como o direito de manter o controle sobre informações pessoais.

A maioria das informações de saúde individualmente identificáveis são informações de saúde protegidas (*Protected Health Information - PHI*), sendo as principais exceções aquelas encontradas em registros de educação (como registros de vacinação) não mantidos por um profissional de saúde, em registros de emprego e informações de saúde de indivíduos falecidos mais do que há 50 anos, pois em caso de falecimento nos últimos 50 anos são consideradas informações de saúde protegidas.

QUESTÕES RELACIONADAS A HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Uma lei federal dos EUA, assinada pelo presidente Bill Clinton em 21 de agosto de 1996, a Lei da Portabilidade e Responsabilização do Seguro de Saúde (*Health Insurance Portability and Accountability Act - HIPAA*) se aplica à maioria dos profissionais da área de saúde, e sua regulamentação, conhecida como Regras de Privacidade (*Privacy Rule*), define regras detalhadas em relação à privacidade, acesso e revelação das informações de saúde individuais identificáveis, conhecidas como informações de saúde protegidas.

A *HIPAA* é uma legislação com os objetivos de ajudar os trabalhadores dos EUA a manter a cobertura do seguro de saúde quando mudam ou perdem empregos, e também busca incentivar os registros eletrônicos de saúde para melhorar a eficiência e a qualidade do sistema por meio de um melhor compartilhamento de informações, proteção, segurança e a privacidade das informações de saúde.

As regras da *HIPAA* se aplicam a planos de saúde, hospitais, prestadores de serviços médicos, instituições de pesquisa e seguradoras que lidam diretamente com pacientes e dados de pacientes.

Atualizações e modificações recentes da *HIPAA* fortaleceram seus padrões e ampliaram a inclusão de quem deve cumprir a *HIPAA*. Fortalecida pela Lei de Tecnologia da Informação em Saúde para Saúde Econômica e Clínica (*Health Information Technology for Economic and Clinical Health - HITECH*), a *HIPAA* reforçou seu rigor com o aumento da auditoria e penalidades, e aplicação severa das leis.

A *HIPAA* se destacou mais após a publicação da Lei *HITECH* em 2009, cujo objetivo era apoiar a implementação nacional de registros eletrônicos de saúde para fornecer dados e informações médicas integradas a provedores e pacientes. A *HITECH* ofereceu programas de incentivo que ajudaram a incentivar a adoção de registros eletrônicos de saúde por hospitais e outros provedores.

O aumento de registros médicos coletados, arquivados e transmitidos eletronicamente levou a desafios em relação à privacidade do paciente.



REGRAS DE PRIVACIDADE (*PRIVACY RULE*)

Em 1999, o Secretário de Saúde e Serviços Humanos propôs a versão inicial da *Privacy Rule* como um conjunto de regras e padrões de proteção da privacidade para o manuseio e transmissão de informações de saúde dos indivíduos, com proibição da venda ou utilização para fins de marketing de informações de saúde protegidas. As regras também incluem Regra de Transações Eletrônicas e Conjuntos de Códigos (*Electronic Transactions and Code Sets Rule*), Requisitos de identificação nacional para empregadores, provedores e planos de saúde (*Employer Identification Number*), e Regra de Segurança (*Security Rule*).

Todas as entidades cobertas pela *HIPAA* devem cumprir a Regra de Segurança. Em geral, esses padrões, requisitos e especificações se aplicam às seguintes entidades cobertas:

Provedores de Saúde Cobertos - Qualquer provedor de serviços ou suprimentos médicos ou de outros cuidados com a saúde que transmita qualquer informação de saúde em formato eletrônico em conexão com uma transação para a qual o Departamento de Saúde e Serviços Humanos tenha adotado um padrão;

Planos de saúde - Qualquer plano individual ou em grupo que forneça ou pague o custo dos cuidados de saúde;

Câmaras de compensação de cuidados de saúde - entidade pública ou privada que processa ou facilita o processamento de elementos de dados não padronizados de informações de saúde em elementos de dados padrão, que realizam serviço de faturação, empresa de reprecificação, sistema de informação de gestão de saúde comunitária ou sistema de informação de saúde comunitária;

Patrocinadores do Cartão de Medicamentos com Prescrição do Medicare – Uma entidade não governamental que oferece um programa de medicamentos com desconto endossado sob a Lei de Modernização do Medicare.

Para fins de pesquisa, pesquisadores podem usar informações de saúde protegidas se receberem autorização dos sujeitos através do Consentimento Informado.

INFORMAÇÕES DE SAÚDE PROTEGIDAS (PHI)

A informação de saúde protegida é qualquer informação pessoal de saúde identificável que é transmitida ou armazenada eletronicamente, como detalhes dos tratamentos de saúde e informação de pagamento que pode identificar um indivíduo. Exemplos:

- Nome;
- Números de segurança social (RG, CPF, dentre outros);
- Datas relacionadas ao cuidado ou tratamento do paciente;
- Datas de nascimento e morte;
- Fotografias;
- Informações de contato;
- Registros de números de exames médicos.

CATEGORIAS DE PROTEÇÕES DA HIPAA

Com a finalidade de garantir a conformidade com a regra de segurança da *HIPAA*, uma organização pode adotar as categorias de proteção:

- Proteção administrativa – como processo de gerenciamento de segurança, atribuição da responsabilidade de segurança, gerenciamento de acesso à informação, treinamento e consciência de segurança, procedimentos de incidentes de segurança;
- Proteção técnica – como controle de acesso e auditoria, autenticação de pessoa ou entidade, transmissão segura;
- Proteção física - controle de acesso físico às instalações, uso da estação de trabalho, controle de dispositivo e mídias.

EXCEÇÕES PARA DIVULGAÇÃO DE INFORMAÇÕES

As informações de saúde protegidas podem ser usadas pelo provedor para fins de cuidado do indivíduo e divulgadas a outros provedores para o mesmo propósito, assim como divulgadas aos serviços de seguro de saúde para notificações de pagamento.

Também podem ser divulgadas a outra pessoa designada pelo indivíduo, como um membro da família, sendo que o mesmo acontece após a sua morte. As divulgações devem sempre ser limitadas ao mínimo.

As instituições podem permitir o acesso dos funcionários apenas aos itens de informações que sejam necessários para o desempenho de suas funções, por exemplo, um funcionário registrado hospitalar pode acessar os nomes e endereços dos pacientes, mas não seus códigos de diagnóstico ou relatórios clínicos.

Como também para atividades e propósitos de saúde pública, como prevenir ou controlar a propagação de doenças ou receber denúncias de abuso ou negligência infantil.

As informações de saúde protegidas podem ser usadas se solicitado por ordem judicial.

TÍTULOS DA HIPAA

A *HIPAA* consiste em 5 seções, chamadas de títulos:

- Título I - diz respeito à proteção à cobertura de seguro saúde para indivíduos que perdem ou mudam de emprego, e proíbe os planos de saúde de negar cobertura a condições preexistentes, a pessoas com doenças específicas e de estabelecer limites de cobertura vitalícia;
- Título II - orienta o Departamento de Saúde e Serviços Humanos dos Estados Unidos a padronizar o processamento de transações eletrônicas de saúde, e exige que as organizações de saúde implementem acesso eletrônico seguro e privativo aos dados de saúde, onde cada entidade de saúde, incluindo indivíduos, empregadores, planos de saúde e fornecedores de saúde, deve ter um número de Identificador de Provedor Nacional exclusivo de 10 dígitos;
- Título III - inclui determinações relacionadas a impostos e diretrizes para cuidados médicos;
- Título IV - define a reforma do seguro de saúde, incorporando disposições para indivíduos com doenças preexistentes e aqueles que buscam cobertura contínua;
- Título V - dispõe sobre seguro de vida de propriedade da empresa e a conduta frente aqueles que perdem sua cidadania americana para fins de imposto de renda.

PRESTADORES DE CUIDADOS DE SAÚDE

Os profissionais de saúde estão mais familiarizados com o título *HIPAA* que aborda a proteção da privacidade e segurança dos registros médicos dos pacientes, pois esta é a parte do *HIPAA* em que os profissionais de saúde recebem treinamento periódico.

Os prestadores de cuidados de saúde têm a obrigação ética e legal de manter a confidencialidade das informações de saúde dos doentes. Assim como de garantir que as informações do paciente sejam divulgadas apenas a indivíduos ou empresas com direito legal de tê-las. Os profissionais de saúde devem usar os dados do paciente apenas para realizar tarefas de trabalho específicas, ou seja, devem usar o mínimo de informações necessárias para cumprir o objetivo da solicitação.

As regras da *HIPAA* ajudam a garantir que qualquer informação divulgada, transmitida ou armazenada pelos provedores e planos de saúde, esteja sujeita a controles de segurança rígidos.

Saiba Mais

Segundo o relatório "*Protected Health Information Data Breach Report*" desenvolvido pela Verizon em 2018, o setor de saúde é o único segmento no qual os funcionários e fornecedores internos representam a maior ameaça de segurança cibernética para toda a organização. Isso mesmo! Entre outras informações, o relatório constatou que 58% dos incidentes cibernéticos em saúde envolvem colaboradores, enquanto a média geral de todos os outros setores é 27%.

Convido você a ler mais sobre o assunto em:

<https://bit.ly/nv71gva> "Proteção de dados sensíveis na saúde", acessado em 15 de agosto de 2022.

<https://bit.ly/715vva8> "Protected Health Information Data Breach Report", acessado em 15 de agosto de 2022.

Privacy Rule (regras de privacidade) tem como objetivo proteger a confidencialidade dos pacientes e suas informações de saúde, permitindo o fluxo de informações de saúde do paciente quando necessário.

A Lei de Tecnologia da Informação em Saúde para Saúde Econômica e Clínica (Lei HITECH) é uma parte da legislação decretada pelo governo dos EUA para promover e impor o uso de tecnologia da informação no setor de saúde; concede aos provedores de saúde incentivos financeiros para a criação de infraestrutura de saúde e manutenção de registros eletrônicos de saúde.

<https://bit.ly/j048gha>

HITECH to 21st century cures: clinician burden and evolving health IT policy. Acessado em 15 de agosto de 2022.

<https://bit.ly/jf18ftgu>

HIPAA Privacy Rule. Acessado em 15 de agosto de 2022.

EM RESUMO

As leis de privacidade e segurança estão evoluindo continuamente para se ajustar a novos desafios, novas tecnologias e novas ameaças na era digital. A Lei da Portabilidade e Responsabilização do Seguro de Saúde (*Health Insurance Portability and Accountability Act - HIPAA*) regula a confidencialidade dos dados clínicos dos pacientes através de *Privacy Rule*, que define regras detalhadas em relação à privacidade, acesso e revelação das informações de saúde individuais identificáveis, conhecidas como informações de saúde protegidas, assim como é uma legislação com os objetivos de ajudar os trabalhadores dos EUA a manter a cobertura do seguro de saúde quando mudam ou perdem empregos.

Aplicação prática

Antes da regulamentação da telemedicina no Brasil e da aprovação da Lei Geral de Proteção de Dados (LGPD), os profissionais brasileiros tinham como referência a *HIPAA*, dos Estados Unidos, que preza pela segurança e criptografia de dados. Hoje, a LGPD é a lei que regulariza o ambiente digital no Brasil, visando eliminar o uso de dados pessoais para fins comerciais sem a autorização do usuário. Por isso, no Brasil, é necessário que as plataformas de telemedicina operem de acordo com a Lei Geral de Proteção de Dados, que impõe uma série de punições para as empresas de tecnologia e prestadoras de serviços médicos que não cumprem as normas.

Acesse: <https://prodoctor.net/blog/devo-ser-hipaa-compliant/>

Na ponta da língua





Referências Bibliográficas

Edemekong, P. F., Annamaraju, P., & Haydel, M. J. (2022). *Health Insurance Portability and Accountability Act*. In StatPearls. StatPearls Publishing.

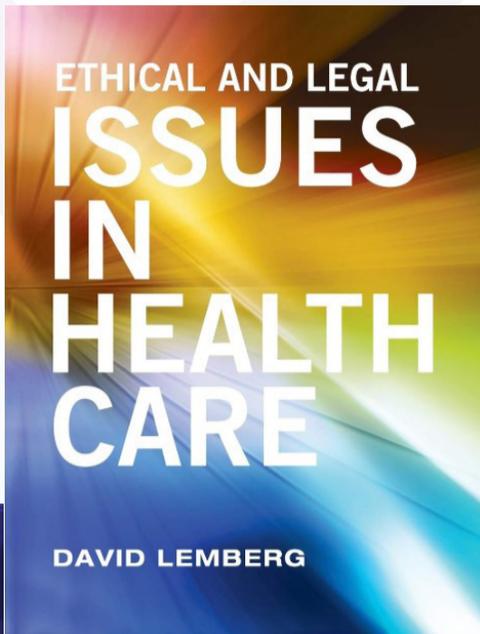
Kayaalp M. (2018). Patient Privacy in the Era of Big Data. *Balkan medical journal*, 35(1), 8–17.

Lemberg, D. (2018). *Ethical and Legal Issues in Healthcare*. Cognella Academic Publishing.

Moore, W., & Frye, S. (2019). Review of *HIPAA*, Part 1: History, Protected Health Information, and Privacy and Security Rules. *Journal of nuclear medicine technology*, 47(4), 269–272.

Williams, K., & Colomb, P. (2020). Important Considerations for the Institutional Review Board When Granting *Health Insurance Portability and Accountability Act* Authorization Waivers. *The Ochsner journal*, 20(1), 95–97.





LIVRO DE REFERÊNCIA:

Ethical and Legal Issues in Healthcare

David Lemberg

Cognella Academic Publishing, 2018.

HIPAA

The Health Insurance Portability and
Accountability Act
of 1996



MUST
UNIVERSITY
FLORIDA - USA