VITRA Health

Capacitação de Cuidadores Edição de Outubro

HIPAA e Privacidade

Resumo da Regra de Segurança da Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA)

Este é um resumo dos principais elementos da regra de segurança, incluindo quem está coberto(a), quais informações são protegidas e quais salvaguardas devem ser implementadas para garantir a proteção adequada das informações eletrônicas de saúde protegidas. Por ser uma visão geral da Regra de Segurança, não aborda todos os detalhes de cada disposição.

Introdução

A Lei de Portabilidade e Responsabilidade de Seguro de Saúde de 1996 (*Health Insurance Portability and Accountability Act*, ou HIPAA, pela sigla em inglês) exigiu que o Secretário do Departamento de Saúde e Serviços Humanos (*U.S. Department of Health and Human Services*, ou HHS, pela sigla em inglês) dos EUA desenvolvesse regulamentos que protegessem a privacidade e a segurança de certas informações de saúde.

Para atender a essa exigência, o HHS publicou o que é comumente conhecido como regra de privacidade da HIPAA e regra de segurança da HIPAA. A Regra de Privacidade, ou Padrões de Privacidade de Informações de Saúde Individualmente Identificáveis (*Standards for Privacy of Individually Identifiable Health Information)*, estabelece padrões nacionais para a proteção de certas informações de saúde. Os Padrões de Segurança para a Proteção de Informações Eletrônicas de Saúde Protegidas (*Security Standards for the Protection of Electronic Protected Health Information)* (a Regra de Segurança) estabelecem um conjunto nacional de padrões de segurança para proteger certas informações de saúde mantidas ou transferidas em formato eletrônico. A regra de segurança operacionaliza as proteções contidas na regra de privacidade, abordando as salvaguardas técnicas e não técnicas que as organizações chamadas “entidades cobertas” devem implementar para proteger as “informações de saúde eletrônicas protegidas” (*electronic protected health information*, ou e-PHI, pela sigla em inglês) dos indivíduos. Dentro do HHS, o Escritório de Direitos Civis (*Office for Civil Rights*, ou OCR, pela sigla em inglês) tem a responsabilidade de fazer cumprir as Regras de Privacidade e Segurança com atividades de conformidade voluntária e penalidades civis em dinheiro.

Antes da HIPAA, não existia nenhum conjunto de padrões de segurança amplamente aceitos ou requisitos gerais para proteger as informações de saúde no setor de saúde. Ao mesmo tempo, novas tecnologias estavam evoluindo e o setor de saúde começou a se afastar dos processos em papel e a depender mais do uso de sistemas eletrônicos de informação para pagar sinistros, responder a perguntas de elegibilidade, dar informações de saúde e desempenhar uma série de outras funções administrativas e de base clínica.

Hoje, os prestadores estão usando aplicativos clínicos, como sistemas computadorizados de registro de ordens médicas (*computerized physician order entry* CPOE, pela sigla em inglês), registros/históricos eletrônicos de saúde (*electronic health records*, ou EHR, pela sigla em inglês) e sistemas de radiologia, farmácia e laboratório. Os planos de saúde oferecem acesso a sinistros e gerenciamento de atendimento, bem como aplicativos de autoatendimento para membros. Embora isso signifique que a força de trabalho médica pode ser mais móvel e eficiente (ou seja, os médicos podem verificar os registros/históricos dos pacientes e os resultados dos exames onde quer que estejam), o aumento na taxa de adoção dessas tecnologias aumenta os possíveis riscos de segurança.

Um dos principais objetivos da regra de segurança é proteger a privacidade das informações de saúde dos indivíduos, permitindo que as entidades abrangidas adotem novas tecnologias para melhorar a qualidade e a eficiência do atendimento aos pacientes. Dado que o mercado de assistência médica é diversificado, a regra de segurança é projetada para ser flexível e escalável para que uma entidade coberta possa implementar políticas, procedimentos e tecnologias que sejam apropriados para o tamanho específico da entidade, estrutura organizacional e riscos para as informações de saúde eletrônicas protegidas (e-PHI) dos consumidores.

Este é um resumo dos principais elementos da regra de segurança e não um guia completo ou abrangente de conformidade. As entidades reguladas pelas Regras de Privacidade e Segurança são obrigadas a cumprir todos os seus requisitos cabíveis e não devem basear-se neste resumo como fonte de informação ou aconselhamento jurídico. Para facilitar a revisão dos requisitos completos da regra de segurança, as disposições da regra mencionadas neste resumo são citadas nas notas finais. Confira a nossa seção de regras de segurança para ver toda a regra e para obter mais informações úteis sobre como a regra se aplica. Em caso de conflito entre este resumo e as Regras, as Regras prevalecerão.

Histórico Regulatório Estatutário

As disposições de Simplificação Administrativa da Lei de Portabilidade e Responsabilidade de Seguro Saúde de 1996 (HIPAA, Título II) exigiam que o Secretário do HHS publicasse padrões nacionais para a segurança de informações de saúde protegidas eletronicamente (e-PHI), envio e recebimento eletrônico, e privacidade e segurança das informações de saúde.

A HIPAA exigiu que o secretário emitisse regulamentos de segurança relativos a medidas para proteger a integridade, confidencialidade e disponibilidade das e-PHI mantidas ou transmitidas pelas entidades cobertas. O HHS desenvolveu uma proposta de regra e a liberou para comentários públicos no dia 12 de agosto de 1998. O Departamento recebeu aproximadamente 2.350 comentários públicos. A regulamentação final, a Regra de Segurança, foi publicada no dia 20 de fevereiro de 2003. A Regra especifica uma série de procedimentos administrativos, técnicos e físicos de segurança a serem usados pelas entidades cobertas para assegurar a confidencialidade, integridade e disponibilidade das e-PHI. O texto do regulamento final pode ser encontrado em 45 CFR Parte 160 e Parte 164, Subpartes A e C.

A quem se aplica a regra de segurança?

A regra de segurança se aplica a planos de saúde, central de informações/câmaras de compensação e liquidação de assistência médica e a qualquer prestador de assistência médica que transmita informações de saúde em formato eletrônico em conexão com uma transação para a qual o Secretário do HHS adotou padrões sob a HIPAA (as “entidades cobertas”) e para seus parceiros de negócios. Para obter ajuda para determinar se você está coberto(a), use a ferramenta de decisão do CMS. Leia mais sobre entidades cobertas no resumo da regra de privacidade da HIPAA.

Parceiros comerciais

A Lei de Tecnologia da Informação em Saúde para a Saúde Clínica e Econômica (*Health Information Technology for Economic and Clinical Health Act*, ou HITECH, pela sigla em inglês) de 2009 ampliou as responsabilidades dos parceiros de negócios sob a Regra de Segurança da HIPAA. O HHS desenvolveu regulamentos para implementar e esclarecer essas mudanças. Veja as orientações adicionais sobre parceiros de negócios.

Quais informações são protegidas?

Informações de saúde protegidas eletronicamente. A regra de privacidade HIPM protege a privacidade de informações de saúde identificáveis individualmente, chamadas informações de saúde protegidas (PHI), conforme explicado na regra de privacidade. A regra de segurança protege um subconjunto de informações cobertas pela regra de privacidade, que são todas as informações de saúde individualmente identificáveis que uma entidade coberta cria, recebe, mantém ou transmite em formato eletrônico. A Regra de Segurança chama essas informações de “informações de saúde protegidas eletronicamente” (e-PHl). A Regra de Segurança não se aplica às PHI transmitidas oralmente ou por escrito.

Regras gerais:

A regra de segurança exige que as entidades cobertas mantenham salvaguardas administrativas, técnicas e físicas razoáveis e apropriadas para proteger as e-PHI. Especificamente, as entidades abrangidas devem:

- Garantir a confidencialidade, integridade e disponibilidade de todas as e-PHI que criarem, receberem, manterem ou transmitirem.
- Identificar e proteger contra ameaças razoavelmente antecipadas à segurança ou integridade das informações.
- Proteger contra usos ou divulgações razoavelmente antecipados e inadmissíveis.

- Assegurar a conformidade por parte de sua força de trabalho.

A regra de segurança define “confidencialidade” de modo que as e-PHI não podem ser disponibilizadas ou divulgadas a pessoas não autorizadas. Os requisitos de confidencialidade da regra de segurança apoiam as proibições da regra de privacidade contra usos e divulgações impróprias das PHI. A regra de segurança também promove os dois objetivos adicionais de manter a integridade e a disponibilidade das e-PHI. De acordo com a regra de segurança, “integridade” significa que as e-PHI não podem ser alteradas ou destruídas sem autorização. “Disponibilidade” significa que as e-PHI podem ser acessadas e usadas sob demanda por uma pessoa autorizada.

O HHS reconhece que as entidades cobertas vão desde o menor prestador até o maior plano de saúde multi-estadual. Assim, a Regra de Segurança é flexível e escalável para permitir que as entidades abrangidas analisem as suas próprias necessidades e implementem soluções adequadas aos seus ambientes específicos. O que é apropriado para uma determinada entidade coberta dependerá da natureza do negócio da entidade coberta, bem como do tamanho e dos recursos da entidade coberta.

Portanto, quando uma entidade coberta está decidindo quais medidas de segurança usar, a Regra não dita essas medidas, mas exige que a entidade coberta avalie:

- Seu tamanho, complexidade e capacidades
- Sua infraestrutura técnica, de hardware e software
- Os custos das medidas de segurança
- A probabilidade e o possível impacto de riscos potenciais para as e-PHl.

Os titulares cobertos devem revisar e modificar suas medidas de segurança para continuar protegendo as e-PHI em um ambiente em constante mudança.

Análise e gerenciamento de riscos

As disposições das Salvaguardas Administrativas na Regra de Segurança exigem que as entidades cobertas realizem análises de risco como parte de seus processos de gestão de segurança. As provisões de análise e gerenciamento de risco da Regra de Segurança são abordadas separadamente aqui porque, ao ajudar a determinar quais medidas de segurança são razoáveis e apropriadas para uma determinada entidade coberta, a análise de risco afeta a implementação de todas as salvaguardas contidas na Regra de Segurança.

Um processo de análise de risco inclui, mas não está limitado às seguintes atividades:

- Avaliar a probabilidade e o impacto de riscos potenciais para as e-PHl.

- Implementar medidas de segurança adequadas para lidar com os riscos identificados na análise de risco.
- Documentar as medidas de segurança escolhidas e, quando necessário, a justificativa para a adoção dessas medidas.
- Manter proteções de segurança contínuas, razoáveis e apropriadas.

A análise de risco deve ser um processo contínuo, no qual uma entidade coberta revisa regularmente seus registros para rastrear o acesso às e-PHI e detectar incidentes de segurança, avaliar periodicamente a eficácia das medidas de segurança implementadas e reavaliar regularmente os riscos potenciais para as e-PHI .

Proteções administrativas

- **Processo de gestão de segurança:** conforme explicado na seção anterior, uma entidade coberta deve identificar e analisar riscos potenciais para as e-PHI e deve implementar medidas de segurança que reduzam riscos e vulnerabilidades a um nível razoável e apropriado.
- **Pessoal de segurança:** uma entidade coberta deve designar um oficial de segurança responsável por desenvolver e implementar suas políticas e procedimentos de segurança.
- **Gestão de acesso à informação:** consistente com o padrão da regra de privacidade que limita os usos e divulgações das PHI ao “mínimo necessário”, a regra de segurança exige que uma entidade coberta implemente políticas e procedimentos para autorizar o acesso às PHI somente quando tal acesso for apropriado com base na função do usuário ou destinatário (acesso baseado em função).
- **Treinamento e gestão do quadro de funcionários:** uma entidade coberta deve providenciar autorização e supervisão adequadas aos membros do quadro de funcionários que trabalham com as e-PHI. Uma entidade coberta deve treinar todos os membros do quadro de funcionários em relação às suas políticas e procedimentos de segurança e deve ter e aplicar as sanções apropriadas contra membros da equipe que violarem suas políticas e procedimentos.
- **Avaliação:** Uma entidade coberta deve realizar uma avaliação periódica de quão bem suas políticas e procedimentos de segurança atendem aos requisitos da Regra de Segurança.

Proteções físicas

- **Acesso e controle das instalações:** uma entidade coberta deve limitar o acesso físico às suas instalações, assegurando ao mesmo tempo que o acesso autorizado seja permitido.
- **Segurança de dispositivos e estações de trabalho:** uma entidade coberta deve implementar políticas e procedimentos para especificar o uso adequado e o acesso a estações de trabalho e mídia eletrônica. Uma entidade coberta também deve ter políticas e procedimentos relativos à transferência, remoção, descarte e reuso de mídia eletrônica

para garantir a proteção apropriada de informações de saúde protegidas eletronicamente (e-PHI).

Proteções Técnicas:

- **Controle de acesso:** uma entidade coberta deve implementar políticas e procedimentos técnicos que permitam que apenas pessoas autorizadas acessem informações eletrônicas protegidas de saúde (e-PHI).
- **Controles de auditoria:** Uma entidade coberta deve implementar hardware, software e/ou mecanismos de procedimento para registrar e examinar o acesso e outras atividades em sistemas de informação que contenham ou usem e-PHI.
- **Controles de integridade:** uma entidade coberta deve implementar políticas e procedimentos para garantir que as e-PHI não sejam alteradas ou destruídas indevidamente. Medidas eletrônicas devem ser implementadas para confirmar que as e-PHI não foram alteradas ou destruídas indevidamente.
- **Segurança de transmissão:** uma entidade coberta deve implementar medidas técnicas de segurança que protegem contra o acesso não autorizado às PHI que estejam sendo transmitidas por uma rede eletrônica.

Requisitos organizacionais

- **Responsabilidades da entidade coberta:** Se uma entidade coberta souber de uma atividade ou prática do parceiro de negócios que constitua uma violação material ou violação da obrigação do parceiro de negócios, a entidade coberta deve tomar medidas razoáveis para remediar a violação ou encerrar a violação. As violações incluem a falha na implementação de salvaguardas que protejam as e-PHI de forma razoável e adequada.
- **Contratos de parceiros comerciais:** o HHS desenvolveu regulamentos relacionados às obrigações e contratos de parceiros comerciais sob a Lei HITECH de 2009.

Requisitos de política, procedimento e documentação

- As entidades cobertas são obrigadas a cumprir todos os “Padrões” da Regra de Segurança. No entanto, a Regra de Segurança categoriza certas especificações de implementação dentro desses padrões como “viáveis”, enquanto outras são “obrigatórias”. As especificações de implementação “obrigatórias” devem ser implementadas. A designação “viáveis” não significa que uma especificação de implementação seja opcional. No entanto, permite que as entidades abrangidas determinem se a especificação de implementação viável é razoável e apropriada para essa entidade abrangida. Caso contrário, a Regra de Segurança permite que a entidade abrangida adote uma medida alternativa que atinja o objetivo da norma se a medida alternativa for razoável e apropriada.

- Atualizações. Uma entidade coberta deve revisar e atualizar periodicamente sua documentação em resposta a mudanças ambientais ou organizacionais que afetem a segurança das informações eletrônicas de saúde protegidas (e-PHI).

Lei estadual

- Preempção. Em geral, as leis estaduais que são contrárias aos regulamentos da HIPAA são preteridas pelos requisitos federais, o que significa que os requisitos federais serão aplicados. “Contrário” significa que seria impossível para uma entidade coberta cumprir simultaneamente os requisitos estaduais e federais, ou que a provisão da lei estadual é um obstáculo para atingir todos os propósitos e objetivos das provisões de Simplificação Administrativa da HIPAA.

Execução e penalidades por descumprimento

- Conformidade: A Regra de Segurança estabelece um conjunto de padrões nacionais de confidencialidade, integridade e disponibilidade das e-PHI. O Escritório de Direitos Civis (OCR) do Departamento de Saúde e Serviços Humanos (HHS) é responsável por administrar e aplicar esses padrões, em conjunto com a aplicação da Regra de Privacidade, e pode fazer investigações de reclamações e revisões de conformidade.

Datas de conformidade:

- Cronograma de conformidade: Todas as entidades cobertas, exceto os “pequenos planos de saúde”, devem estar em conformidade com a Regra de Segurança até 20 de abril de 2005. Os pequenos planos de saúde tinham até 20 de abril de 2006 para cumprir.

Cópias da Regra e materiais relacionados

- Para mais materiais de orientação, consulte a seção "Combined Regulation Text of All Rules" (Texto Regulamentar Consolidado de Todas as Regras) em nosso site para obter o conjunto completo de regulamentações de simplificação administrativa da HIPAA e sobre a HIPAA para profissionais.

Fonte: www.hhs.gov