O Departamento de Saúde e Serviços Humanos dos EUA emitiu uma proposta de regra em 6 de janeiro para melhorar a segurança cibernética e proteger melhor o sistema de saúde dos EUA contra um número crescente de ataques cibernéticos.

As últimas alterações propostas à Lei de Portabilidade e Responsabilidade de Seguros de Saúde representam as primeiras grandes atualizações do departamento desde 2013, abordando alguns dos desafios mais prementes de segurança cibernética. No entanto, também destacam áreas onde é necessária mais inovação para proteger informações sensíveis dos pacientes num mundo cada vez mais interligado.

Se finalizadas, estas alterações imporão requisitos mais rigorosos às entidades cobertas pela HIPAA — tais como prestadores de cuidados de saúde e seguradoras — e aos seus parceiros comerciais, enfatizando medidas proativas de segurança cibernética. As partes interessadas são incentivadas a analisar as alterações propostas e enviar comentários até 7 de março.

O que você vai ler:

Novas medidas visam proteger a segurança dos dados — mas as empresas ainda têm trabalho a fazer

A proposta de regra de segurança da HIPAA introduz medidas obrigatórias que refletem a crescente sofisticação das ameaças cibernéticas. Isso inclui criptografia de ponta a ponta, que garante que as informações eletrônicas de saúde protegidas permaneçam ilegíveis para usuários não autorizados durante todo o seu ciclo de vida. A autenticação multifator também se tornou obrigatória para sistemas que contêm ePHI, equilibrando a segurança robusta com as demandas operacionais dos ambientes clínicos.

Além disso, o monitoramento contínuo substituiria as avaliações periódicas de risco, permitindo que as organizações identificassem e abordassem proativamente ameaças

potenciais por meio de sistemas automatizados que rastreiam o acesso e mantêm registros de auditoria detalhados. Embora estas medidas reforcem as defesas, centram-se principalmente nos sistemas internos, deixando lacunas nas interações de terceiros e nas práticas globais de partilha de dados.

VEJA: Grupo de ameaças cibernéticas ligado à China hackeia o Departamento do Tesouro dos EUA

Lidando com riscos de terceiros

Os ecossistemas modernos de cuidados de saúde dependem da partilha de conteúdos confidenciais com fornecedores, subcontratantes e colaboradores de investigação. No entanto, esta abordagem introduz riscos substanciais.

A pesquisa mostra que quase quatro em cada 10 organizações de saúde compartilham conteúdo confidencial com 2.500 ou mais terceiros. Sistemas centralizados com criptografia e controles de acesso são essenciais para gerenciar as trocas de dados com segurança. Essas plataformas fornecem visibilidade sobre o tratamento de dados externos, ao mesmo tempo que aplicam medidas de segurança consistentes.

Acordos claros com terceiros são essenciais para mitigar riscos, descrevendo protocolos de segurança específicos, respostas a violações e requisitos de relatórios. Auditorias regulares e monitoramento em tempo real fortalecem ainda mais as defesas, ajudando as organizações a detectar e resolver vulnerabilidades prontamente. Mesmo uma violação menor numa entidade pode expor toda a rede a ameaças significativas sem tais medidas.

As colaborações globais de investigação acrescentam outra camada de complexidade, exigindo alinhamento com padrões internacionais como o GDPR. As políticas que protegem a partilha transfronteiriça de dados garantem que as informações sensíveis são protegidas em todas as jurisdições, permitindo que as organizações mantenham a conformidade e a colaboração num cenário de cuidados de saúde interligados.

Cobertura de segurança de leitura obrigatória

Aproveitando a IA para conformidade e segurança cibernética

A inteligência artificial tem um potencial transformador para a segurança cibernética, mas a sua integração na conformidade com a HIPAA permanece pouco explorada.

A IA pode monitorar sistemas em tempo real, detectar anomalias no compartilhamento de arquivos e e-mails, transferência de arquivos e outros canais de comunicação de conteúdo

confidencial, e analisar dados históricos para antecipar e combater ameaças emergentes. A modelagem preditiva de ameaças e as ferramentas automatizadas de conformidade simplificam a documentação e geram insights acionáveis.

São necessárias normas regulamentares claras para aproveitar o potencial da IA. Isto inclui protocolos de validação e diretrizes éticas para sua implantação. A integração de soluções baseadas em IA com estruturas de segurança existentes melhorará a conformidade e criará uma defesa dinâmica e adaptativa contra ameaças cibernéticas em evolução.

VEJA: Linha do tempo: 15 ataques cibernéticos e violações de dados notáveis

Como a IA desempenha um papel na detecção e no combate às ameaças cibernéticas

A monitorização em tempo real melhorou significativamente a segurança dos dados, mas a sua eficácia depende da integração de tecnologias avançadas. Os registos de auditoria centralizados são cruciais, oferecendo uma visão consolidada do acesso e das alterações aos dados, o que apoia a monitorização contínua e a resposta a incidentes. Ao manter registros detalhados, as organizações podem detectar e resolver anomalias rapidamente.

A IA desempenha um papel fundamental no aprimoramento desses esforços. Algoritmos de aprendizado de máquina analisam riscos dinamicamente, identificando vulnerabilidades potenciais antes que elas aumentem. A IA também pode detectar padrões indicativos de uso indevido de dados ou colaboração não autorizada, garantindo a mitigação proativa de ameaças. Além disso, a tecnologia blockchain complementa estes esforços, fornecendo registos imutáveis que aumentam a transparência e a responsabilização.

Juntas, estas inovações criam uma estrutura robusta para monitorização contínua, tornando os sistemas mais resilientes a ataques cibernéticos sofisticados.

Preenchendo as lacunas na conformidade

Apesar do progresso, persistem vários desafios de conformidade. Os fornecedores mais pequenos enfrentam frequentemente dificuldades na criação de documentação abrangente devido aos recursos limitados. A ausência de padrões de referência padronizados em toda a indústria leva a inconsistências, enquanto a falta de estruturas de relatórios uniformes complica os processos de auditoria.

Os registos de auditoria centralizados são fundamentais para colmatar estas lacunas. Os registros de auditoria fornecem insights claros e práticos sobre o acesso, uso e possíveis vulnerabilidades de dados, consolidando todas as atividades relacionadas à conformidade em um único sistema. Esses registros permitem que as organizações simplifiquem os relatórios, garantam a consistência e simplifiquem as auditorias de conformidade, oferecendo uma visão transparente e em tempo real de todas as atividades.

Para melhorar ainda mais a conformidade, as organizações devem adotar plataformas que integrem ferramentas e painéis de relatórios automatizados com esses registros de auditoria. Avaliações em tempo real e análises baseadas em IA podem identificar anomalias e ajudar a prevenir violações de conformidade. A colaboração com fornecedores de tecnologia confiáveis também pode resultar em soluções personalizadas que abordam desafios específicos de segurança e conformidade.

Ao centralizar o gerenciamento de conformidade e aproveitar a tecnologia, as organizações de saúde podem construir estruturas escaláveis que se alinhem com os requisitos regulatórios e melhorem a proteção geral dos dados.

Amplos benefícios da segurança cibernética centrados no paciente

Medidas mais rigorosas de segurança cibernética fazem mais do que prevenir violações; eles promovem a confiança.

É mais provável que os pacientes se envolvam com fornecedores comprometidos em proteger seus dados. Esta confiança apoia inovações mais amplas, como a medicina personalizada e a monitorização da saúde em tempo real, melhorando, em última análise, a qualidade dos cuidados. As organizações de saúde podem alcançar eficiência operacional priorizando a segurança cibernética e construindo relacionamentos duradouros com seus pacientes.

As últimas alterações da HIPAA marcam um passo importante na abordagem dos desafios de segurança cibernética dos cuidados de saúde. No entanto, à medida que o cenário digital evolui, a inovação contínua é imperativa. Os registos de auditoria centralizados e as análises baseadas em IA devem desempenhar um papel fundamental na transformação da conformidade numa iniciativa proativa e estratégica. Essas ferramentas permitem que as organizações detectem, investiguem e respondam a incidentes em tempo real, transformando obrigações regulatórias em pontos fortes operacionais.

No futuro, as organizações de saúde devem priorizar a integração de tecnologias avançadas para antecipar ameaças emergentes. A mudança de medidas reativas para estratégias proativas aumenta a segurança e aumenta a confiança dos pacientes e a resiliência operacional. Aqueles que agirem de forma decisiva na adopção destas inovações estarão mais bem equipados para enfrentar os desafios futuros e navegar pelas complexidades de um ecossistema de cuidados de saúde cada vez mais interligado.

Patrick Spencer é vice-presidente de marketing corporativo e pesquisa da Kiteworks.