FOXIT ESIGN – ÜBERSICHT ÜBER DIE HIPAA-KONFORMITÄT

WHITEPAPER

INHALTSVERZEICHNIS

EINFÜHRUNG

Die Umstellung auf elektronische Daten ist in vollem Gange. Eine effizientere Kommunikation von Informationen zwischen Gesundheitsdienstleistern und die Forderung nach einer besseren Patientenerfahrung haben zu einer umfassenderen Einführung digitaler Prozesse für die Bearbeitung von Patientenakten geführt. Mit der höheren Effizienz, die digitale Prozesse mit sich bringen, geht jedoch auch eine intensive Kontrolle einher. Die Weitergabe und der Verkauf vertraulicher Informationen wie der Gesundheitsdaten von Patienten ist für Hacker attraktiv und hat verheerende Folgen. Die Verwaltung von Patientendaten unterliegt daher einer strengen Verordnung, die als HIPAA (Health Insurance Portability and Accountability Act) bezeichnet wird. Gesundheitsdienstleister und Unternehmen der Gesundheitsbranche müssen Wege finden, um die von den Patienten erwartete effiziente Versorgung zu gewährleisten, ohne die ihnen anvertrauten Gesundheitsdaten zu missbrauchen.

Dieses Dokument bietet einen Überblick über die HIPAA-Verordnung und deren Auswirkungen auf Ihre Organisation. Es beantwortet auch einige der häufigsten Fragen im Zusammenhang mit der Verwendung elektronischer Dokumente im Gesundheitswesen und zeigt, wie Foxit eSign diese Herausforderungen meistert.

WAS IST HIPAA UND DIE DATENSCHUTZREGEL?

HIPAA (Health Insurance Portability and Accountability Act) ist eine umfassende US-Gesundheitsverordnung, die 1996 erlassen wurde. Ursprünglich wurde das Gesetz unterzeichnet, um die Übertragbarkeit und Rechenschaftspflicht von Krankenversicherungen zu verbessern. Seither wurde HIPAA jedoch weiterentwickelt, um die Vertraulichkeit von Patienten zu schützen. Titel II des HIPAA enthält die „Standards für den Datenschutz von individuell identifizierbaren Gesundheitsdaten“ (Standards for Privacy of Individually Identifiable Health Information) oder einfach die „Datenschutzregel“, die eine Reihe von Standards für den Schutz von Gesundheitsdaten festlegt. Die Datenschutzregel regelt die Verwendung und Weitergabe geschützter Gesundheitsdaten (Protected Health Information, PHI) durch die betroffenen Einrichtungen, zu denen Gesundheitsdienstleister, Krankenkassen und Clearingstellen für das Gesundheitswesen gehören.

Der Schutz von Gesundheitsdaten wurde inzwischen durch zwei Gesetze erweitert. Mit dem HITECH Act von 2009 wurde der Schutz auf die Übertragung elektronischer Aufzeichnungen und Daten ausgedehnt. Mit der HIPAA Omnibus-Regel von 2013 wurden die Schutzanforderungen auf Geschäftspartner ausgedehnt. Ein Geschäftspartner ist eine natürliche oder juristische Person, die bestimmte Funktionen oder Tätigkeiten ausführt, die die Verwendung oder Offenlegung von geschützten Gesundheitsdaten im Namen einer betroffenen Einrichtung beinhalten. Nach diesen Vorschriften müssen von HIPAA betroffene Einrichtungen, die mit Anbietern oder Auftragnehmern zusammenarbeiten möchten, eine Geschäftspartnervereinbarung (Business Associate Agreement, BAA) abschließen, damit deren Produkte und/oder Dienstleistungen den Schutz und die Sicherheit von geschützten Gesundheitsdaten in Übereinstimmung mit HIPAA gewährleisten.

WAS GILT ALS GESCHÜTZTE GESUNDHEITSDATEN IM SINNE VON HIPAA?

HIPAA definiert geschützte Gesundheitsdaten (Protected Health Information, PHI) als alle Gesundheitsdaten, die sich im Gewahrsam einer betroffenen Einrichtung befinden und die zur Identifizierung eines Patienten verwendet werden können. Im Grunde genommen gelten alle Informationen über den Patienten als geschützte Gesundheitsdaten. Geschützte Gesundheitsdaten sind Informationen, die beispielsweise in Krankenakten, Krankengeschichten, Laborergebnissen und Krankenversicherungsrechnungen zu finden sind. Zu den 18 individuellen Identifikationsmerkmalen, die laut HIPAA als geschützte Gesundheitsdaten eingestuft werden, gehören unter anderem die folgenden:

Namen	Kontaktnummern	Nummern von Krankenakten
Sozialversicherungsnummern	Adressen (physisch und E-Mail)	Geburtsdaten
Geschlecht	Medizinische Vorgeschichte	Impfpass

WELCHES SIND BETROFFENE EINRICHTIGUNGEN IM SINNE DER DATENSCHUTZREGEL?

Zu den von HIPAA betroffenen Einrichtungen gehören unter anderem die folgenden:

Gesundheitsdienstleister	Krankenkassen	Clearingstellen für das Gesundheitswesen
• Ärzte • Kliniken • Zahnärzte • Psychologen • Apotheken • Augenoptiker • Chiropraktiker • Medizinische Spezialisten • Pflegeheime	• Krankenversicherungsgesellschaften • HMOs • Betriebskrankenkassen • Medicare • Medicaid • COBRA	Jede öffentliche oder private Einrichtung, die Gesundheitsdaten in einem Standardformat verarbeitet oder deren Verarbeitung ermöglicht (oder umgekehrt) • Abrechnungsdienste • Preisfestsetzungsunternehmen • Gemeinschaftliche Gesundheitsinformationssysteme • Gemeinschaftliche Gesundheitsmanagementsysteme

Die Datenschutzregel verlangt auch, dass die betroffenen Einrichtungen von den Geschäftspartnern ausreichende Zusicherungen erhalten, dass der Geschäftspartner die geschützten Gesundheitsdaten, die er im Namen der betroffenen Einrichtung erhält oder erstellt, angemessen schützen wird.

Zu den Geschäftspartnern gehören unter anderem:

- Anwaltskanzleien oder Buchhaltungsfirmen
- Software-Anbieter
- Hersteller medizinischer Geräte
- Abrechnungsunternehmen
- Web-Hosts

Wenn Ihre Organisation eine von HIPAA betroffene Einrichtung ist, müssen Sie sicherstellen, dass alle in Ihrem Besitz befindlichen geschützten Gesundheitsdaten sowie die zu Geschäftszwecken mit Ihren Geschäftspartnern ausgetauschten geschützten Gesundheitsdaten vollständig geschützt sind, um die Vorschrift einzuhalten. Sie müssen

unbedingt beachten, dass die betroffene Einrichtung vor dem Abschluss einer Vereinbarung mit Geschäftspartnern sicherstellen muss, dass sie über ein angemessenes Compliance-Programm verfügt, und die Fähigkeit des Geschäftspartners, die Anforderungen von HIPAA an den Schutz von geschützten Gesundheitsdaten zu erfüllen, vollständig überprüfen muss.

Foxit eSign ist ein Anbieter von Lösungen für elektronische Datentransaktionen und kann verschlüsselte geschützte Gesundheitsdaten auf seinen Servern übertragen und aufbewahren, was ihn als Geschäftspartner qualifiziert. Foxit eSign bietet Vereinbarungen für Geschäftspartner (Business Associate Agreements, BAA) mit betroffenen Einrichtungen im Rahmen der Pro- und Enterprise-Tarife an.

GILT HIPAA AUCH FÜR NICHT-US-ORGANISATIONEN?

Nein, HIPAA gilt nur für Organisationen des Gesundheitswesens in den USA. Alle Personen, die einem US-Gesundheitssystem angehören, sind durch die Verordnung geschützt, auch diejenigen, die keine US-Bürger sind. Umgekehrt fallen US-Bürger, die einer Gesundheitseinrichtung außerhalb der USA angehören, nicht unter HIPAA.

WELCHES SIND HÄUFIGE HIPAA-VERSTÖSSE?

HIPAA-Verstöße sind schwerwiegend und können mit Strafen von bis zu 50.000 USD pro Verstoß und einer maximalen jährlichen Strafe von bis zu 1,5 Millionen USD pro Verstoß belegt werden. Noch schwerwiegender ist, dass Sammelklagen von Betroffenen die entsprechenden Einrichtungen lahmlegen können. Daher ist es für die betroffenen Einrichtungen unerlässlich, die Einhaltung von HIPAA in der Praxis sicherzustellen. Da die meisten Informationen hauptsächlich elektronisch übermittelt werden, ergeben sich einige der häufigsten HIPAA-Verstöße aus der unsachgemäßen Weitergabe oder Offenlegung von Daten. Dies sind häufige Beispiele:

- Unverschlüsselte Daten – Elektronische Dateien mit unverschlüsselten geschützten Gesundheitsdaten können zu einer Datenschutzverletzung führen.
- Datenschutzverletzung – Schwache Schutzmaßnahmen oder Sicherheitslücken sind anfällig für Hackerangriffe und können zur illegalen Offenlegung von Patientendaten führen.
- Unbefugter Zugriff – Es ist wichtig, dass nur die Personen, die auf Patientendaten zugreifen müssen, auch dazu in der Lage sind. Jede Person, die außerhalb dieser Anforderung auf die geschützten Patientendaten zugreift, verstößt gegen die Vorschrift.
- Entsorgung von geschützten Patientendaten – Selbst das Löschen elektronischer geschützter Patientendaten ohne die entsprechenden Methoden könnte die Daten für Hacker angreifbar machen.

Foxit eSign wird jährlich von einer HIPAA-Compliancy-Firmengruppe geprüft, um die Zusammenarbeit mit den betroffenen Einrichtungen zu ermöglichen. Alle elektronischen geschützten Gesundheitsdaten werden sicher verschlüsselt und von der Quelle direkt an unsere sicheren Server übertragen. Alle Daten sind im Hintergrund und bei der Übertragung vollständig geschützt.

WIE ERFÜLLT FOXIT ESIGN DIE HIPAA-ANFORDERUNGEN?

Foxit eSign ist als HIPAA-konform zertifiziert, um sicherzustellen, dass der Umgang mit den privaten und vertraulichen Dokumenten Ihrer Patienten stets den Vorschriften entspricht. Für den Schutz der Gesundheitsdaten stellt Foxit eSign sichere Felder zur Verfügung, um diese Informationen zu verbergen. Wir verwenden Verschlüsselung und Tokenisierung, um die Weitergabe von geschützten Gesundheitsdaten zu verhindern. Alle Daten werden im Hintergrund und bei der Übertragung verschlüsselt. Jede Signaturtransaktion mit Foxit eSign enthält einen vollständig rückverfolgbaren, fälschungssicheren Prüfpfad und wird mit einem Abschlusszertifikat versehen.

Die in unseren SOC2-geprüften Rechenzentren gespeicherten Dokumente werden mit dem AES-256-Standard auf der Anwendungsebene für Kundendokumente verschlüsselt, um absolute Vertraulichkeit zu gewährleisten.

Darüber hinaus werden mit Foxit eSign die HIPAA-Bestimmungen wie folgt erfüllt:

- Rechtsverbindliche elektronische Signaturen (gemäß UETA und ESIGN), die den gesetzlichen Anforderungen standhalten
- Strenge Einhaltung der HIPAA-Standards für die Sicherheit und den Schutz elektronischer Daten
- Detaillierte Dokumentationsstandards, die Quellen- und Identitätsüberprüfung, Verschlüsselungsschlüssel, Hash-Algorithmen zum Sperren von Dokumenten und andere Signaturtechnologien zur Unterstützung der Einhaltung von Vorschriften umfassen
- Gesicherter Zugriff auf Dokumente und gesicherte Übertragung von Dokumenten
- Umfassende Prüfung, die die Übertragung und Unterzeichnung jedes Dokuments verfolgt
- Detaillierte Protokolle, um den detaillierten Aktivitätsverlauf jeder Interaktion einschließlich des Standorts der Beteiligten, die auf die Dokumente zugreifen, vor und nach der Unterzeichnung des Dokuments bereitzustellen

INFORMATIONEN ZU FOXIT ESIGN

Foxit eSign ist eine rechtsverbindliche Lösung für elektronische Signaturen, mit der Sie wichtige digitale Dokumente vorbereiten, versenden, unterzeichnen und verwalten können. Laden Sie Ihr Dokument einfach hoch, erstellen Sie Ihre Vorlage, fügen Sie Empfänger hinzu und übermitteln Sie das Dokument zum Unterzeichnen. API-Arbeitsabläufe können sowohl für direkte Unterschriften als auch für absenderbasierte elektronische Signaturen einfach eingerichtet werden. Foxit eSign automatisiert die Arbeitsabläufe und bietet einen nahtlosen Prozess, der es dem Benutzer ermöglicht, Signaturvorgänge im Browsers zu senden, zu signieren, zu verfolgen und zu verwalten. Nach der Ausfertigung haben Sie ein fälschungssicheres und rechtsgültig unterzeichnetes Dokument, das für praktisch jeden Zweck verwendet werden kann. Darüber hinaus wird das elektronische Signieren noch weiter vereinfacht, da Absender und Unterzeichner von jedem Ort der Welt aus, an dem eine Internetverbindung verfügbar ist, und mit praktisch jedem Gerät arbeiten können.

Foxit
Lennéstr. 1
10785 Berlin, Deutschland

Vertrieb: +49 30 234849944
oder +49 30 234849945
Support: +49 30 21783691

Support Center
www.foxit.com