Datenschutz- und Sicherheitsrichtlinie

Schutz und Sicherheit von personenbezogenen und gesundheitsbezogenen Daten haben für Outcome Sciences, Inc., auch „Outcome“ genannt, höchste Priorität. Outcome schützt vertrauliche personenbezogene und gesundheitsbezogene Daten, die es von Geschäftspartnern und freiwilligen Studienteilnehmern sowie medizinischem Fachpersonal und medizinischen Einrichtungen, die einen Datenbestand pflegen, erhalten hat, mit aller Sorgfalt. Outcome verpflichtet sich, die anwendbaren gesetzlichen Bestimmungen, Regeln und Vorschriften bei der Nutzung, Erfassung und Weitergabe dieser Daten einzuhalten. Diese Datenschutz- und Sicherheitsrichtlinie ist ein dynamisches Dokument und gibt so wieder, dass wir kontinuierlich unsere besondere Aufmerksamkeit darauf richten, die Informationen, mit deren Verwaltung wir vertraut wurden, ordnungsgemäß zu behandeln und zu sichern.

I. Für Benutzer in den Vereinigten Staaten gelten die Bestimmungen dieses Abschnitts I:

Der Health Insurance Portability and Accountability Act von 1996 („HIPAA“) und die gemäß dem HIPPA eingeführten Regeln und Vorschriften wurden zum Schutz gesundheitsbezogener Informationen erlassen, die sich auf einzelne Personen zurückführen lassen; dieser Schutz umfasst Datenschutz, Sicherheit und Weitergabe. Organisationen im Gesundheitswesen, zu denen Health Plans und Leistungsanbieter gehören, müssen den HIPPAA einhalten; bei Nichteinhaltung drohen erhebliche Sanktionen durch das Department of Health and Human Services, die US-Regierungsbehörde, die zur Durchsetzung des HIPAA befugt ist. Die Einhaltung des HIPAA ist in vielerlei Hinsicht wichtig, da der HIPAA rechtliche sowie die Aufsicht, Verfahren, Sicherheit und Technologie betreffende Anforderungen angibt, die Organisationen im Gesundheitswesen auferlegt werden, welche mit auf einzelne Personen zurückführbaren gesundheitsbezogenen Informationen umgehen.

Outcome ist zwar keine Organisation im Gesundheitswesen, aber bestimmte im HIPAA angegebene Verpflichtungen gelten für Outcome, wenn wir als Geschäftspartner (Business Associate nach der Definition im HIPAA) für Organisationen im Gesundheitswesen tätig sind, wenn Outcome beispielsweise Forschungsstudien nach der Marktfreigabe und Programme zur Qualitätsverbesserung an verschiedenen Standorten im Gesundheitswesen durchführt; diese Tätigkeiten umfassen die Nutzung und Weitergabe von gesundheitsbezogenen Daten, die sich auf einzelne Personen zurückführen lassen. Outcome verpflichtet sich, auf einzelne Personen zurückführbare gesundheitsbezogene Informationen in Übereinstimmung mit US-amerikanischen Bundesgesetzen und -verordnungen zu behandeln, die die Sicherheit und den elektronischen Umgang mit geschützten gesundheitsbezogenen Daten betreffen; dies umfasst, ist aber nicht beschränkt auf anwendbare HIPAA-Anforderungen zu Sicherheit und elektronischer Übertragung und weitere gesetzliche Verfügungen.

Alle Lösungen von Outcome für die Forschung nach der Markteinführung entsprechen dem HIPAA und sind auf die vorhandenen HIPAA-Protokolle von Organisationen im Gesundheitswesen abgestimmt. Outcome besitzt umfangreiche Erfahrungen bei der Anpassung von Produkten für Organisationen im Gesundheitswesen und Pharmaunternehmen und arbeitet eng mit ihnen zusammen, um die Einhaltung des HIPAA durch die Organisationen im Gesundheitswesen zu unterstützen. Outcome hat branchenweit die größte Anzahl von webbasierten Studien und Registern entwickelt und verwaltet, und unsere Online-Systeme werden in mehr 2.000 Krankenhäusern in den USA verwendet, darunter alle größeren Universitätskliniken.

Outcome hat administrative, strukturelle und technische Sicherheitsvorkehrungen getroffen, die die Vertraulichkeit, Integrität und Verfügbarkeit elektronisch geschützter gesundheitsbezogener Daten auf vernünftige und angemessene Weise schützen. Outcome verwaltet Sicherheit mit strukturellen und logischen Methoden. Unsere Systeme und Datenbanken werden in einer sicheren und überwachten Einrichtung mit Zugangskontrolle verwaltet. Zu den von uns eingesetzten Mechanismen gehören Verschlüsselung, Authentifizierung, Angriffserkennung, Benutzeridentifizierung, sichere Speicherung und Sicherung, Schwärzung von Daten und nicht veränderbare Protokolle. Darüber hinaus wird die Systemsicherheit regelmäßig von unabhängigen externen Experten bewertet.

Zusammenfassend lässt sich feststellen, dass die Systeme von Outcome nach hohen Standards für die Erfassung, den Umgang und die Übertragung von Informationen im Gesundheitswesen verwaltet werden. Wir verfolgen regelmäßig technische, verfahrenstechnische und gesetzliche Änderungen, die sich auf den Schutz geschützter gesundheitsbezogener Daten auswirken.

II. Für Benutzer in der Europäischen Union gelten die Bestimmungen dieses Abschnitts II:

Nach EU-Gesetzgebung sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person „personenbezogene Daten". Personenbezogene Daten müssen in Übereinstimmung mit dem Rechtsrahmen gespeichert werden, der in der Datenschutzrichtlinie 95/46/EG (der „Datenschutzrichtlinie") vorgegeben ist. Alle personenbezogenen Daten werden bei Vorliegen einer Einverständniserklärung oder gemäß den Genehmigungen der entsprechenden Ethikkommissionen in einer sicheren Datenbank gespeichert. Alle Mitarbeiter von Outcome, die mit personenbezogenen Daten umgehen, erhalten Schulungen zu den Anforderungen der einschlägigen Gesetze und Verordnungen. Outcome verpflichtet sich, sicherzustellen, dass personenbezogene medizinische Daten (als sensible Daten) streng vertraulich behandelt werden; personenbezogene Daten dürfen jedoch an Aufsichtsbehörden weitergegeben werden, um behördliche Genehmigungen zu erhalten oder um die anwendbaren rechtlichen Anforderungen einzuhalten. Personenbezogene Daten dürfen außerdem in Übereinstimmung mit den Einverständniserklärungen der betroffenen Personen, deren personenbezogene Daten für Forschungen verwendet werden können, oder wie anderweitig durch Genehmigungen entsprechender Ethikkommissionen zulässig, an bestimmte Dritte weitergegeben werden. Personenbezogene Daten dürfen in manchen Fällen auch verschlüsselt werden; bei der Nutzung der verschlüsselten Daten werden die in den EU-Datenschutzgrundsätzen angegebenen Verfahren eingehalten. Einzelpersonen sind berechtigt, auf Anfrage ihre gespeicherten personenbezogenen Daten einzusehen und zu korrigieren.

Das US-Handelsministerium und die Europäische Kommission haben eine Reihe von Datenschutzgrundsätzen und häufig gestellten Fragen vereinbart, damit US-Unternehmen die im EU-Recht niedergelegten Anforderungen an den angemessenen Schutz von personenbezogenen Daten erfüllen können, die von der EU in die Vereinigten Staaten übertragen werden (die „Safe Harbor Principles"). Der Europäische Wirtschaftsraum („EWR") hat ebenfalls anerkannt, dass die Safe Harbor Principles einen angemessenen Schutz persönlicher Daten bieten. Zum EWR gehören die fünfundzwanzig Mitglieder der Europäischen Union sowie Island, Liechtenstein und Norwegen. Outcome verpflichtet sich, personenbezogene Daten zu schützen, und befolgt die Safe Harbor Principles in Bezug auf Informationspflicht, Wahlmöglichkeit, Datenweitergabe, Datenauskunftsrecht, Sicherheit, Datenintegrität und Durchsetzung.

Wenn Outcome personenbezogene Daten unmittelbar von Einzelpersonen im EWR erfasst, informiert das Unternehmen sie über den Zweck der Erfassung und Nutzung ihrer personenbezogenen Daten, nämlich die Durchführung von Studien, die ihre personenbezogenen Daten beinhalten können. Outcome gibt Daten nur an beauftragte Dritte weiter, um die Dienste von Outcome in Übereinstimmung mit den oben beschriebenen Grundsätzen auszuführen. Outcome kann personenbezogene Daten an seine Niederlassung in den USA weitergeben, an Beauftragte, die dem US-amerikanischen Gesetz zum Schutz gesundheitsbezogener Daten unterliegen (dem Health Insurance Portability and Accountability Act von 1996 („HIPAA")), und an Beauftragte, die nicht dem HIPAA unterliegen. Für die Weitergabe an Niederlassungen von Outcome in den USA oder an Beauftragte, die nicht dem HIPAA unterliegen, liegen aber im Falle von Outcome geeignete Zusicherungen vor und werden auch von den Beauftragten von Outcome angefordert. Diese Zusicherungen können Folgendes umfassen: einen Vertrag, der den Beauftragten verpflichtet, zumindest den Schutz zu bieten, wie er von den relevanten Safe Harbor Principles gefordert wird, oder die Angabe, dass der Beauftragte der Safe Harbor-Zertifizierung nach EU-Richtlinie 95/46/EG oder einer anderen, von der Europäischen Kommission als gleichwertig angesehenen Zertifizierung unterliegt (beispielsweise der Safe Harbor-Zertifizierung zwischen der Schweiz und den USA).

Outcome erkennt die Wichtigkeit an, den Schutz von online erfassten und/oder gespeicherten Daten zu erhalten, und verfügt über Systeme, die die online oder über eine elektronische Datenbank erfassten und/oder gespeicherten Daten schützen. Outcome hat administrative, strukturelle und technische Sicherheitsvorkehrungen getroffen, um elektronische personenbezogene Daten vor Verlust, missbräuchlicher Verwendung und unerlaubtem Zugriff zu schützen. Outcome verfolgt insbesondere die Zertifizierung gemäß den internationalen Sicherheitsstandards BS ISO/IEC 27001:2005 für Informationsmanagementsysteme. Diese Standards setzen die OECD-Richtlinien über Datenschutz, Datensicherheit und Netzwerksysteme um.

Um den bestmöglichen Standard für das System zur Erfassung und Übertragung medizinischer Daten beizubehalten, verfolgt Outcome die Änderungen in Bezug auf technische, behördliche und gesetzgeberische Standards für den Schutz und die Sicherheit personenbezogener Daten.

III. Für Benutzer außerhalb der Vereinigten Staaten und außerhalb der Europäischen Union gelten die Bestimmungen dieses Abschnitts III:

Outcome stellt sicher, dass alle personenbezogenen Daten, die es von einem beliebigen Ort auf internationaler Ebene erhält, ordnungsgemäß und in Übereinstimmung mit den internationalen Datenschutzregeln, die für diese personenbezogenen Daten gelten, aufbewahrt werden. Outcome beabsichtigt, dass seine Standardverfahren bei der Erfassung, Nutzung und Weitergabe von personenbezogenen Daten mit den lokalen Datenschutzgesetzen, soweit anwendbar, übereinstimmen. Die Richtlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung („OECD") über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten (die „OECD-Richtlinien") stellen allgemeine Grundsätze des Datenschutzes dar. Diese OECD-Richtlinien sind grundlegender Bestandteil der meisten internationalen Datenschutzgesetze. Um einen hohen Schutz für personenbezogene Daten zu gewährleisten, die von Outcome aufbewahrt und verarbeitet werden, werden diese Daten von Outcome gemäß den in den OECD-Richtlinien angegebenen Standards erfasst, genutzt und weitergegeben.

Alle personenbezogenen Daten werden mit Einverständnis der betroffenen Person oder gemäß anderer geeigneter Genehmigungen in einer sicheren Datenbank gespeichert. Alle Mitarbeiter von Outcome, die mit personenbezogenen Daten umgehen, erhalten Schulungen zu den Anforderungen der Datenschutzgesetze und -verordnungen. Outcome verpflichtet sich, sicherzustellen, dass personenbezogene Daten streng vertraulich behandelt werden; personenbezogene Daten dürfen jedoch an Aufsichtsbehörden weitergegeben werden, um gemäß den geltenden rechtlichen Anforderungen behördliche Genehmigungen zu erhalten oder um sonstigen geltenden rechtlichen Anforderungen nachzukommen. Personenbezogene Daten dürfen außerdem in Übereinstimmung mit den eindeutigen Einverständniserklärungen der betroffenen Personen, deren personenbezogene Daten für Forschungen verwendet werden können, oder wie anderweitig durch entsprechende Genehmigungen zulässig, an bestimmte Dritte weitergegeben werden. Personenbezogene Daten dürfen in manchen Fällen auch verschlüsselt werden; bei der Verwendung der verschlüsselten Daten werden die in den OECD-Richtlinien angegebenen Verfahren eingehalten. Einzelpersonen sind berechtigt, auf Anfrage ihre gespeicherten personenbezogenen Daten einzusehen und zu korrigieren.

Wenn Outcome auf internationaler Ebene personenbezogene Daten unmittelbar von Einzelpersonen erfasst, informieren wir sie über den Zweck der Erfassung und Nutzung ihrer personenbezogenen Daten, nämlich die Durchführung von Studien, die ihre personenbezogenen Daten beinhalten können, und andere relevante Zwecke. Outcome darf Daten nur an beauftragte Dritte weitergeben, um die Dienste von Outcome in Übereinstimmung mit den oben beschriebenen Grundsätzen auszuführen. Outcome kann personenbezogene Daten an seine Niederlassungen in den USA weitergeben, die diese Daten gemäß dieser Richtlinie aufbewahren. Outcome kann personenbezogene Daten zudem an beauftragte Personen übertragen; von ihnen werden geeignete Zusicherungen angefordert, dass die personenbezogenen Daten in Übereinstimmung mit den OECD-Richtlinien und lokal geltendem Recht behandelt werden.

Outcome erkennt die Wichtigkeit an, den Schutz von online erfassten und/oder gespeicherten Daten zu erhalten, und verfügt über Systeme, die die online oder über eine elektronische Datenbank erfassten und/oder gespeicherten personenbezogenen Daten schützen. Outcome hat administrative, strukturelle und technische Sicherheitsvorkehrungen getroffen, um elektronische personenbezogene Daten vor Verlust, missbräuchlicher Verwendung und unerlaubtem Zugriff zu schützen. Outcome verfolgt insbesondere die Zertifizierung gemäß den internationalen Sicherheitsstandards BS ISO/IEC 27001:2005 für Informationsmanagementsysteme. Diese Standards setzen die OECD-Richtlinien über Datenschutz, Datensicherheit und Netzwerksysteme um.

Um den bestmöglichen Standard für das System zur Erfassung und Übertragung von Daten beizubehalten, verfolgt Outcome die Entwicklungen in Bezug auf technische, behördliche und gesetzgeberische Standards für den Schutz und die Sicherheit personenbezogener Daten.