

## **Política de privacidad y seguridad de los datos**

La privacidad y seguridad de los datos personales y la información médica es una cuestión prioritaria para Outcome Sciences, Inc., que opera bajo la denominación comercial de Outcome (“Outcome”). Outcome protege cuidadosamente la información personal y médica confidencial que le proporcionan sus asociados comerciales, los sujetos voluntarios participantes en investigaciones, los profesionales sanitarios y las instituciones sanitarias que almacenan y actualizan los datos. Outcome se compromete a cumplir la legislación, las normas y las regulaciones aplicables en cuanto al uso, recopilación y divulgación de dicha información. Esta Política de privacidad y seguridad de los datos es un documento dinámico que reflejará nuestra permanente atención con respecto al manejo y la protección de la información cuyo mantenimiento nos ha sido confiado.

### **I. Los términos de esta Sección I se aplican a los usuarios residentes en los Estados Unidos:**

La ley Health Insurance Portability and Accountability Act de 1996 (“HIPAA”, Ley de Responsabilidad y Portabilidad de Seguros Médicos), así como las normas y regulaciones que se aprobaron en el marco de la HIPAA, están destinadas a proteger la privacidad, seguridad y distribución de información sanitaria que permita la identificación de personas. Las organizaciones de asistencia sanitaria, entre las que se incluyen compañías de seguros médicos y proveedores de asistencia sanitaria, deben cumplir la ley HIPAA so pena de enfrentarse a graves sanciones del U.S. Department of Health and Human Services (Departamento de Salud y Servicios Humanos de EE.UU.), la agencia gubernamental encargada del cumplimiento de la HIPAA. El cumplimiento de la HIPAA tiene una importancia de amplio alcance, ya que la HIPAA especifica los requisitos legales, normativos, procedimentales, de seguridad y tecnológicos impuestos a las organizaciones de atención sanitaria que manejan información sanitaria que permite la identificación de personas.

Aunque Outcome no es una organización de atención sanitaria, algunos deberes y obligaciones de la HIPAA se aplican a Outcome cuando actúa en calidad de Asociado Comercial (según se define en la HIPAA) de organizaciones de atención sanitaria, como por ejemplo, cuando Outcome facilita la realización de estudios de investigación posteriores a la autorización de venta y programas de mejora de calidad en distintos centros de atención sanitaria, lo que implica el uso y la divulgación de información sanitaria que permite la identificación de personas. Outcome se compromete a manejar la información sanitaria que permita la identificación de personas de conformidad con la normativa y legislación federales de los EE.UU. relativas a la seguridad y el manejo electrónico de la información sanitaria protegida, incluidos, sin limitación, los requisitos aplicables de la HIPAA sobre seguridad y transferencia electrónica, así como cualquier otro mandato legal.

Todas las soluciones de investigación poscomercialización de Outcome cumplen la HIPAA y se adaptan a los protocolos HIPAA existentes en las organizaciones de atención sanitaria. Outcome tiene una amplia experiencia en la adaptación de productos para organizaciones de atención sanitaria y empresas farmacéuticas, y ha trabajado estrechamente con ellas para facilitar el cumplimiento de la HIPAA por parte de las organizaciones de atención sanitaria. Outcome ha desarrollado y gestionado el mayor número de estudios y registros electrónicos del sector, y nuestros sistemas en línea se utilizan en más de 2.000 hospitales de los EE.UU., incluidos todos los grandes centros académicos.

Outcome ha puesto en práctica medidas de protección administrativas, físicas y técnicas para proteger razonable y adecuadamente la confidencialidad, integridad y disponibilidad de la información sanitaria electrónica protegida. Outcome gestiona la seguridad a través de métodos físicos y lógicos. Nuestros sistemas y bases de datos se encuentran en instalaciones protegidas, supervisadas y con un estricto control de acceso. Entre los mecanismos que empleamos se encuentran el cifrado, la autenticación, la detección de intrusiones, la identificación de usuarios, el almacenamiento seguro con copias de seguridad, la ocultación de datos y las trazas de auditoría no modificables. Además, una empresa experta e independiente realiza periódicamente evaluaciones externas de la seguridad de nuestros sistemas.

En resumen, el mantenimiento de los sistemas de Outcome se realiza conforme a los más altos estándares de recopilación, manejo y transmisión de información sanitaria. Supervisamos periódicamente los cambios tecnológicos, procedimentales y normativos que afectan a la protección de la información sanitaria protegida.

## **II. Los términos de esta Sección II se aplican a los usuarios residentes en la Unión Europea:**

Según la legislación de la UE, toda información relacionada con una persona física identificada o identificable se considera “datos personales”. Los datos personales se deben conservar de conformidad con el marco legal dispuesto en la Directiva de Protección de Datos 95/46/EC (la “Directiva de Protección de Datos”). Con el consentimiento del titular de la información o de acuerdo con otras autorizaciones de los comités éticos pertinentes, todos los datos personales se almacenan en una base de datos segura. Todo el personal de Outcome encargado de manejar información personal recibe formación específica sobre los requisitos de las leyes y normativas aplicables. Outcome se compromete a garantizar la estricta confidencialidad de la información médica personal (como datos sensibles); no obstante, los datos personales podrán revelarse a las autoridades normativas con el fin de obtener su autorización o para cumplir con los requisitos legales pertinentes. Los datos personales también podrán divulgarse a determinadas terceras partes, siempre de acuerdo con los términos establecidos en los consentimientos informados obtenidos de los sujetos cuyos datos personales puedan utilizarse para labores de investigación, o bien de otro modo si así lo permiten otras autorizaciones de los comités éticos pertinentes. Además, en ocasiones, los datos personales podrán codificarse y, si se utilizan, el método de codificación se tratará de forma coherente con los principios de protección de datos de la UE. Los titulares de la información podrán acceder a sus datos personales y corregirlos si así lo desean.

El Departamento de Comercio de los Estados Unidos y la Comisión Europea han acordado un conjunto de principios y preguntas frecuentes sobre la protección de datos, con el fin de que las empresas estadounidenses puedan cumplir los requisitos normativos de la Unión Europea a la hora de transferir información personal desde la UE a los EE.UU. (los “Principios de puerto seguro”). El Espacio Económico Europeo (“EEE”) también reconoce que los Principios de puerto seguro proporcionan una protección adecuada para los datos personales. El EEE incluye a los veinticinco países miembros de la Unión Europea más Islandia, Liechtenstein y Noruega. Outcome se compromete a proteger la privacidad de la información personal y cumple los Principios de puerto seguro relativos a la notificación, elección, transferencia de información, acceso a la información personal, seguridad, integridad de los datos y aplicación.

Cuando Outcome recopile datos personales directamente de personas del EEE, informará a dichas personas de los fines con los que recopilará y utilizará tales datos; a saber, la realización de investigaciones en las que puedan emplearse sus datos personales. Outcome únicamente proporcionará información a terceros con el fin de ofrecer los servicios de Outcome de acuerdo con los principios anteriormente citados. Outcome puede transferir datos personales a sus sedes en los Estados Unidos, a agentes sujetos a la normativa federal sobre protección de información sanitaria de los Estados Unidos (la Ley de Responsabilidad y Portabilidad de Seguros Médicos de 1996, “HIPAA”) y a agentes que no estén sujetos a la HIPAA. No obstante, en lo que respecta a las transferencias a las sedes de Outcome en los Estados Unidos o a agentes que no están sujetos a la HIPAA, Outcome ha adoptado las garantías oportunas y las exige también a los agentes. Tales garantías pueden incluir: un contrato que obligue al agente a proporcionar como mínimo el mismo nivel de protección que exigen los Principios de puerto seguro relevantes, supeditación del agente a la certificación Puerto seguro de la Directiva Europea 95/46/EC o supeditación del agente a otra medida de idoneidad de la Comisión Europea (por ejemplo, la Certificación de Puerto seguro Suiza-EE.UU.).

Outcome reconoce la importancia de mantener la privacidad de la información recopilada o almacenada en línea y cuenta con sistemas que protegen los datos recopilados y/o almacenados en línea o a través de una base de datos electrónica. Outcome ha implementado medidas de protección administrativas, físicas y técnicas para impedir la pérdida y el uso indebido de los datos personales en formato electrónico, así como el acceso no autorizado a los mismos. En concreto, Outcome se halla en proceso de obtener el certificado de las normas internacionales de seguridad BS ISO/IEC 27001:2005 relativas a los sistemas de gestión de la información. Estas normas aplican las directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre privacidad, seguridad de la información y sistemas de red.

Con el fin de mantener los más altos estándares en nuestro sistema de recopilación y transmisión de información, Outcome mantiene un seguimiento continuo de los cambios que se producen en los estándares tecnológicos, normativos y legislativos en lo que respecta a la privacidad y seguridad de los datos personales.

### **III. Los términos de esta Sección III se aplican a los usuarios residentes fuera de los Estados Unidos y la Unión Europea:**

Es intención de Outcome garantizar que todos los datos personales que se le faciliten, provenientes de cualquier lugar del mundo, se traten adecuadamente y de conformidad con la normativa internacional de protección de datos que sea de aplicación a tales datos personales. Outcome pretende que sus prácticas y procedimientos estándar en lo relativo a la recopilación, el uso y la divulgación de datos personales se atengan a las leyes locales de protección de datos, donde proceda. Las directrices de la Organización para la Cooperación y el Desarrollo Económico (“OCDE”) sobre la protección de la privacidad y el flujo transfronterizo de datos personales (las “directrices de la OCDE”) establecen principios generales sobre privacidad. Estas directrices de la OCDE constituyen el núcleo de la mayoría de leyes sobre protección de datos de todo el mundo. Para garantizar un alto nivel de protección de la información personal que Outcome conserva y procesa, Outcome recopilará, utilizará y divulgará los datos personales de conformidad con los estándares establecidos por las directrices de la OCDE.

Con el consentimiento del sujeto o de acuerdo con otras autorizaciones pertinentes, todos los datos personales se almacenan en una base de datos segura. Todo el personal de Outcome encargado de manejar información personal recibe formación específica sobre los requisitos normativos relacionados con la protección de datos. Outcome se compromete a garantizar la estricta confidencialidad de los datos personales; no obstante, los datos personales podrán revelarse a las autoridades normativas con el fin de obtener su autorización de acuerdo con los requisitos legales pertinentes, o bien para cumplir con estos de alguna otra forma. Los datos personales también podrán divulgarse a determinadas terceras partes, siempre de acuerdo con los términos inequívocos establecidos en los consentimientos informados obtenidos de los sujetos cuyos datos personales puedan utilizarse para labores de investigación, o bien de otro modo si así lo permiten otras autorizaciones pertinentes. Además, en ocasiones, los datos personales podrán codificarse y, si se utilizan, el método de codificación se tratará de forma coherente con las directrices de la OCDE. Los titulares de la información podrán acceder a sus datos personales y corregirlos si así lo desean.

Cuando Outcome recopile datos personales directamente de personas de todo el mundo, informará a dichas personas de los fines con los que recopilará y utilizará tales datos; a saber, la realización de investigaciones en las que puedan emplearse sus datos personales y cualesquiera otros fines relevantes. Outcome únicamente proporcionará información a terceros con el fin de ofrecer los servicios de Outcome de acuerdo con los principios anteriormente descritos. Outcome puede transferir datos personales a sus oficinas de los Estados Unidos, y estas oficinas conservarán esos datos de acuerdo con esta política. Outcome también puede transferir información personal a agentes, de quienes se exigirán las garantías adecuadas para asegurar que dicha información personal se tratará de acuerdo con las directrices de la OCDE y las leyes locales pertinentes.

Outcome reconoce la importancia de mantener la privacidad de la información recopilada o almacenada en línea y cuenta con sistemas que protegen los datos personales recopilados y/o almacenados en línea o a través de una base de datos electrónica. Outcome ha implementado medidas de protección administrativas, físicas y técnicas para impedir la pérdida y el uso indebido de los datos personales en formato electrónico, así como el acceso no autorizado a los mismos. En concreto, Outcome se halla en proceso de obtener el certificado de las normas internacionales de seguridad BS ISO/IEC 27001:2005 relativas a los sistemas de gestión de la información. Estas normas aplican las directrices de la OCDE sobre privacidad, seguridad de la información y sistemas de red.

Con el fin de mantener los más altos estándares en nuestro sistema de recopilación y transmisión de información, Outcome mantiene un seguimiento continuo de los desarrollos que se producen en los estándares tecnológicos, normativos y legislativos en lo que respecta a la privacidad y seguridad de los datos personales.