

Personvern- og sikkerhetspolicy

Personvern og sikkerheten av personlige data og helseinformasjon er av primært anliggende for Outcome Sciences, Inc. d/b/a Outcome ("Outcome"). Outcome er nøye med å beskytte fortrolig personlig og helseinformasjon som er gitt av forretningspartnere og frivillige forskningspersoner, helsearbeidere og helseinstitusjoner som fører data. Outcome er forpliktet til følgende gjeldende lover, regler og forskrifter i vår bruk, innsamling og videresending av slik informasjon. Denne datapersonvern- og sikkerhetspolicyen er et dynamisk dokument, som vil avspeile vår vedvarende årvåkenhet for å håndtere og sikre informasjon på riktig måte som er betrodd oss.

I. For brukere som befinner seg i USA, skal vilkår i dette Avsnitt I gjelde:

Health Insurance Portability and Accountability Act of 1996 ("HIPAA") og reglene og forskriftene som er implementert under HIPAA var vedtatt for å beskytte personvern, sikkerhet og distribusjonen av individuelt identifiserbar helseinformasjon. Helseorganisasjoner, som inkluderer helseplaner og leverandører av helsetjenester, må overholde HIPAA eller møte betydelige sanksjoner fra det amerikanske Helsedepartementet, det statlige organet som er autorisert til å håndheve HIPAA. Overholdelse av HIPAA er av omfattende betydning fordi HIPAA spesifiserer juridiske, regulerende, prosess-, sikkerhets- og teknologiske krav pålagt helseorganisasjoner som behandler individuelt identifiserbar helseinformasjon.

Selv om Outcome ikke er en helseorganisasjon, gjelder enkelte av HIPAAs forpliktelser Outcome når vi fungerer som forretningsforbindelse (som definert under HIPAA) av helseorganisasjoner, som når Outcome fasiliteter utførelse av ettermarkeds-studier for godkjenningssforskning og kvalitetsforbedringsprogrammer ved forskjellige helseinstitusjoner, som involverer bruk og videreføring av individuelt identifiserbar helseinformasjon. Outcome er forpliktet til å håndtere individuelt identifiserbar helseinformasjon på en måte som er i samsvar med amerikanske lover og forskrifter om sikkerhet og elektronisk behandling av beskyttet helseinformasjon, inkludert, men ikke begrenset til, gjeldende HIPAA-krav til sikkerhet og elektronisk overføring, og alle andre juridiske mandater.

Alle Outcomes løsninger for ettermarkedsføringsstudier er i samsvar med HIPAA og griper inn i helseorganisasjoners eksisterende HIPAA-protokoller. Outcome har omfattende erfaring med å tilpasse produkter for helseorganisasjoner og legemiddelprodusenter, og har jobbet tett sammen med dem for å fasilitere helseorganisasjoners overholdelse av HIPAA. Outcome har utviklet og administrert det største antallet webbaserte eStudier og eRegistre i industrien, og våre onlinek-systemer brukes på mer enn 2000 sykehus i USA, inkludert hvert sentrale akademiske senter.

Outcome har implementert administrative, fysiske og tekniske sikkerhetsanordninger som beskytter konfidensialiteten, integriteten og tilgjengeligheten av elektronisk beskyttet helseinformasjon på en rimelig og passende måte. Outcome administrerer sikkerhet gjennom både fysiske og logiske metoder. Våre systemer og databaser opprettholdes på et sikkert, tilgangskontrollert og overvåket anlegg. Mekanismene vi benytter inkluderer kryptering, autentisering, inntrengerdeteksjon, brukeridentifisering, sikker lagring og backup, dataredigering og ikke-modifiserbare revisjonsspor. Eksterne evalueringer av systemsikkerheten utføres også rutinemessig av en uavhengig, ekspert-tredjepart.

Til oppsummering, vedlikeholdes Outcomes systemer i henhold til høye standarder for innsamling, behandling og overføring av informasjon til helsevesen. Vi overvåker regelmessig teknologiske, prosedyremessige og lovbestemte endringer som påvirker beskyttelsen av beskyttet helseinformasjon.

II. For brukere som befinner seg i EU, skal vilkår i dette Avsnitt II gjelde:

I henhold til EU-lovgivning, er all informasjon som gjelder en identifisert eller identifiserbar naturlig person "personlig data". Personlig data må holdes i samsvar med det juridiske rammeverket som fremgår av Data Protection Directive 95/46/EC (Dataverndirektivet). Med samtykke eller i overensstemmelse med godkjenninger fra egnede etiske komiteer, lagres alle personlige data på en sikker database. Alt personale i Outcome som behandler personlig data får opplæring i kravene i gjeldende lover og forskrifter. Outcome er forpliktet til å sikre at personlig helseinformasjon (som sensitiv data) oppbevares strengt konfidensielt. Men personlig data kan videresendes til regulerende myndigheter med henblikk på å skaffe deres godkjenning, eller for å overholde gjeldende juridiske krav. Personlig data kan også videresendes til enkelte tredjeparter i samsvar med vilkårene til et informert samtykke fra datasubjekter hvis personlige data kan brukes til forskningsaktiviteter, eller som ellers tillatt av godkjenninger fra gjeldende etiske komiteer. Personlig data kan til tider også være nøkkelkodet. Hvis de i så fall brukes, behandles metoden for nøkkelkoding i samsvar med prinsippene bak EU-datavern. Individer har rett til å få tilgang til og korrigere personlig data om dem hvis de ønsker det.

Det amerikanske Handelsdepartementet og EU er blitt enige om et sett med datavernprinsipper og ofte stilte spørsmål for å gjøre det mulig for amerikanske bedrifter å oppfylle kravet i henhold til EU-lovgivning om at tilstrekkelig beskyttelse blir gitt til personlig informasjon som sendes fra EU til USA ("Safe Harbor Principles"). EØS har også anerkjent at Safe Harbor Principles har gitt tilstrekkelig beskyttelse til personlige data. EEA inkluderer de tjue-fem medlemmene av EU pluss Island, Liechtenstein og Norge. Outcome er forpliktet til å beskytte personvern og overholder Safe Harbor Principles i forhold til å gi varsel, valgmulighet, videreføring av informasjon, tilgang til personlig informasjon, sikkerhet, dataintegritet og overholdelse.

Der Outcome samler inn personlig data direkte fra individer i EEA, vil de informere dem om formålet som dataene samles for og brukes til, nemlig gjennomføring av forskning som kan involvere deres personlige data. Outcome vil gi informasjon til tredjepartsagenter med henblikk på å gi Outcomes tjenester på en måte som er i samsvar med prinsippene som er nevnt overfor. Outcome kan overføre personlig data til sitt amerikanske kontor, til agenter som er gjenstand for amerikansk nasjonal lov i forhold til beskyttelsen av helseinformasjon (Health Insurance Portability and Accountability Act of 1996 ("HIPAA")), så vel som agenter som ikke er underlagt HIPAA. Ved overføringer til Outcomes kontorer i USA eller til agenter som ikke er underlagt HIPAA, derimot, er aktuelle sikkerheter på plass når det gjelder Outcome, og søkes fra Outcomes agenter. Disse sikkerhetene kan inkludere: en kontrakt som forplikter agenten til å gi minst samme nivå av beskyttelse som kreves av de aktuelle Safe Harbor Principles, som er underlagt EU-direktiv 95/46/EC Safe Harbor-sertifisering av agenten, eller som er underlagt et annet EU-krav (f.eks. Swiss-US Safe Harbor Certification).

Outcome innser betydningen av å opprettholde personvern for informasjon som er innhentet og/eller lagret online og har systemer på plass som beskytter data som er innhentet og/eller lagret online eller via en elektronisk database. Outcome har implementert administrative,

fysiske og tekniske sikkerhetstiltak for å beskytte elektronisk personlig data fra tap, misbruk og uautorisert tilgang. Outcome søker spesielt om sertifisering etter de internasjonale sikkerhetsstandardene BS ISO/IEC 27001:2005 for informasjonsbehandlingssystemer. Disse standardene implementerer Organisasjonen for økonomisk samarbeid og utviklings retningslinjer for personvern, informasjonssikkerhet og nettverkssystemer.

For å opprettholde vårt informasjonsinnsamlings- og overføringssystem til optimale standarder, overvåker Outcome endringer i teknologiske, regulerende og juridiske standarder i forhold til personvern og sikkerhet av personlig data.

III. For brukere som befinner seg utenfor USA og utenfor EU, skal betingelsene i dette Avsnitt III gjelde:

Det er Outcomes intensjon å sikre at alle personlige data som er gitt, uansett hvor fra i verden, ivaretas på passende måte og i samsvar med internasjonale datavernregler som gjelder slike personlige data. Outcome har til hensikt at deres standardpraksis og -prosedyrer i forhold til innhenting, bruk og videreføring av personlige data vil samsvare med lokale datavernlover, der det er aktuelt. Retningslinjene til Organization for Economic Co-operation and Development ("OECD") om beskyttelse av personvern og internasjonal datatrafikk av personlig data ("OECD-retningslinjene") fremsetter generelle prinsipper for personvern. Disse OECD-retningslinjene utgjør kjernen i de fleste globale datavernlovene. For å sikre høy standard av beskyttelse for personlig informasjon som oppbevares og behandles av Outcome, vil personlig data samles, brukes og videresendes av Outcome i samsvar med standardene som fremgår av OECD-retningslinjene.

Med samtykke av data underlagt eller i henhold til andre egnede godkjenninger, lagres alle personlige data på en sikker database. Alt personale i Outcome som behandler personlig data får opplæring i kravene i datavern-relaterte lover og forskrifter. Outcome er forpliktet til å sikre at personlig data oppbevares strengt konfidensielt. Men personlig data kan videresendes til regulerende myndigheter med henblikk på å skaffe deres godkjenning i samsvar med gjeldende juridiske krav, eller for på annen måte å overholde gjeldende juridiske krav. Personlig data kan også videresendes til enkelte tredjeparter i samsvar med vilkårene til et utvetydig informert samtykke fra datasubjekter hvis personlige data kan brukes til forskningsaktiviteter, eller som ellers tillatt av godkjenninger fra andre. Personlig data kan til tider også være nøkkelkodet. Hvis de i så fall brukes, behandles metoden for nøkkelkoding i samsvar med OECD-retningslinjene. Individuer har rett til å få tilgang til og korrigere personlig data om dem hvis de ønsker det.

Der Outcome samler inn personlig data direkte fra individer over hele verden, vil vi informere dem om formålet som dataene samles for og brukes til, nemlig gjennomføring av forskning som kan involvere deres personlige data og eventuelle andre relevante formål. Outcome vil gi informasjon til tredjepartsagenter med henblikk på å gi Outcomes tjenester på en måte som er i samsvar med prinsippene som er beskrevet overfor. Outcome kan overføre personlige data til sine amerikanske kontorer, og de kontorene vil oppbevare slike data i samsvar med denne policyen. Outcome kan også overføre personlig informasjon til agenter som passende sikkerhet vil søkes fra for at den personlige informasjonen vil behandles i samsvar med OECD-retningslinjer og gjeldende lokale lover.

Outcome innser betydningen av å opprettholde personvern for informasjon som er innhentet og/eller lagret online og har systemer på plass som beskytter data som er innhentet og/eller lagret online eller via en elektronisk database. Outcome har implementert administrative, fysiske og tekniske sikkerhetstiltak for å beskytte elektronisk personlig data fra tap, misbruk og uautorisert tilgang. Outcome søker spesielt om sertifisering etter de internasjonale sikkerhetsstandardene BS ISO/IEC 27001:2005 for informasjonsbehandlingssystemer. Disse standardene implementerer OECDs retningslinjer om personvern, informasjonssikkerhet og nettverkssystemer.

For å opprettholde vårt informasjonsinnsamlings- og overføringssystem til optimale standarder, overvåker Outcome endringer i forhold til teknologiske, regulerende og juridiske standarder i forhold til personvern og sikkerhet av personlig data.