Bijlage B2 – Databeveiliging

Voor de uitvoer van het DDD-partnership verwerkt i2i grote hoeveelheden privacy- en marktgevoelige informatie van zowel verzekeraars als zorgverleners. Om de veiligheid van deze informatie te waarborgen, gaat i2i zeer zorgvuldig om met de data en data-uitwisseling.

i2i maakt gebruik van een TTP voor de data-aanleveringen. Dit is Stichting Beheer Pseudonimisatie Doelmatig Direct Declareren Partnership (hierna: Stichting DDD of SBPDDDP), bestuurd door Zivver, gevestigd te Amsterdam aan de Overschiestraat 186.-J (KvK-nr: 64894665), e-mail: info@doelmatigdirectdeclareren.nl. Stichting DDD is onafhankelijk van i2i opgericht en staat buiten de invloedsfeer van i2i. De Stichting is een dedicated Trusted Third Party en heeft als enig doel om data op een veilige manier te versleutelen en anonimiseren.

Zowel i2i als Zivver zijn in het bezit van het ISO 27001 certificaat en werken volgens de NEN 7510 standaard. Op hoofdlijnen worden de maatregelen die i2i toepast hier nader toegelicht.

Dataverzameling en gegevensoverdracht

In overleg met zorgverleners en verzekeraar wordt vastgesteld welke data periodiek verzonden dienen te worden aan i2i (via SBPDDDP). Deze data doorloopt vervolgens 3 stappen voordat deze bij i2i terecht komt (zie onderstaande schematische weergave).

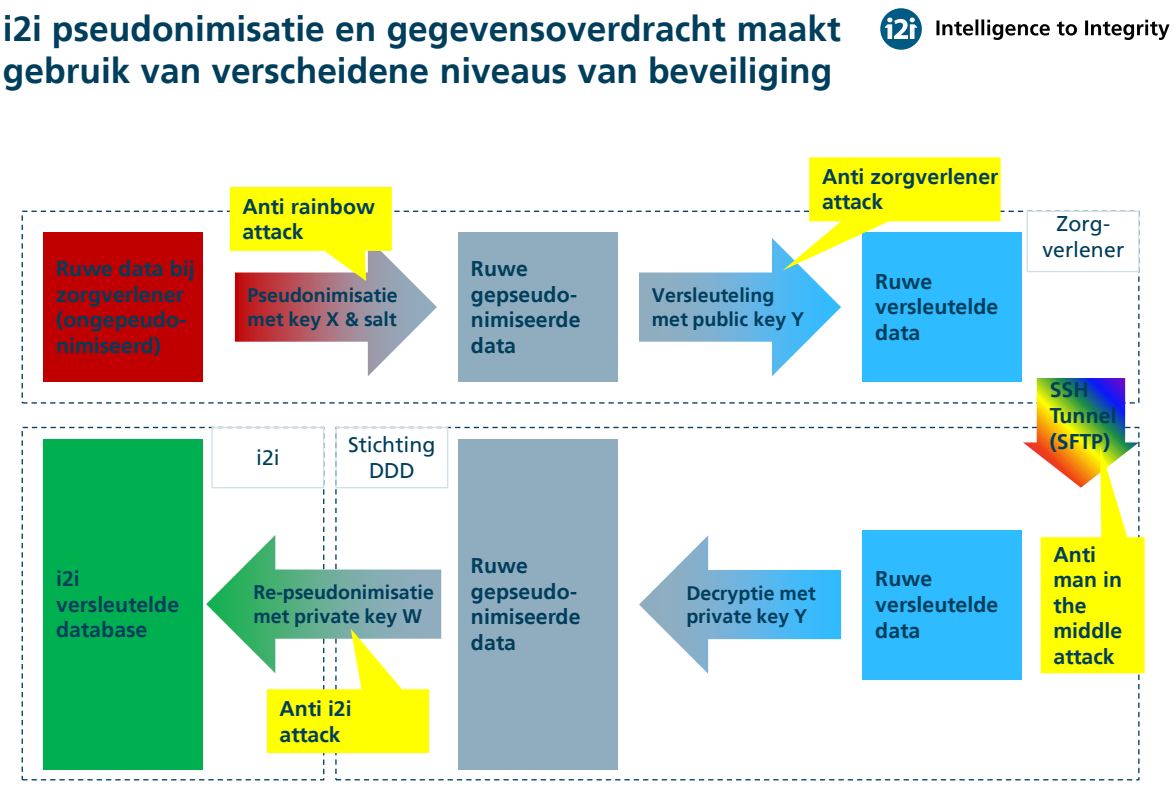
1) De dataset wordt lokaal bij de zorgverlener of verzekeraar gepseudonimiseerd en versleuteld met programmatuur die Stichting DDD ter beschikking stelt. Deze programmatuur is geaudit door Deloitte (rapport op verzoek beschikbaar) en bewerkt de data als volgt:

   A) Anonimisering door verschillende maatregelen (combinatie van pseudonimisering en hashing, verwijdering, generalisatie en aggregatie):
      a) Versleuteld BSN en verzekerdennummer van de patiënt onomkeerbaar tot een identificerende “hash” (HMAC-SHA1 incl. dubbele salt en key)
      b) Reduceert geboortedatum tot geboortejaar
      c) Reduceert postcode tot alleen cijfers en aggregeert kleine postcodes (<200)
      d) Landcode buitenland wordt geagregeerd tot één code
      e) Verwijderd patiëntennummer bij instelling en factuurnummer
      f) Laat alle overige patiëntgegevens weg (bijv. adres, woonplaats, etc.)
   B) Versleuteling:
      a) Versleuteld data cryptografisch met public key, zodat deze alleen met private key door Stichting DDD ontsleuteld kan worden.

2) De geanonimiseerde en versleutelde data kan de contactpersoon van i2i bij de verzekeraar of zorgverlener via het beveiligde Stichting DDD intranet uploaden – indien gewenst kan ook dit proces geautomatiseerd worden. Het DDD intranet maakt gebruik van een volledig beveiligde en versleutelde verbinding: 128/256-bit SSL encryptie op basis van een digitaal COMODO certificaat. Middels een unieke login en password combinatie wordt toegang verkregen tot de upload portal van het DDD intranet. Via de portal is uitsluitend het uploaden van bestanden mogelijk. Downloaden of andere bestanden inzien is om veiligheidsredenen onmogelijk gemaakt.

3) Binnen de Stichting DDD wordt de data ontsleuteld tot ruwe geanonimiseerde data. Vervolgens worden alle pseudoniemen nogmaals gepseudonimieerd met een aparte sleutel voordat de data aangeboden wordt aan i2i.

Zodoende komt i2i nooit in contact met herleidbare persoonskenmerken en is een i2i werknemer, stichting DDD werknemer, of zorgverlener werknemer zelfs met kwade opzet niet in staat de data-aanlevering te herleiden tot individuele patiënten.



IT-infrastructuur

De data-aanleveringen die binnenkomen bij Stichting DDD en i2i worden opgeslagen op data-acceptatie servers. Deze (en alle gegevensdragers) zijn beveiligd met 256-bit AES encryptie. Daarnaast zijn deze servers uitgerust met een geavanceerde dubbele firewall (router en server level).

Als de data uiteindelijk binnenkomt op de acceptatie-server van i2i wordt deze fysiek naar de interne database servers verplaatst (“Olympus” en “Delphi”), aangezien deze servers fysiek gescheiden zijn van het internet. Na verplaatsing naar Olympus en Delphi blijven er geen data-aanleveringen achter op de data-acceptatie servers.

Om de veiligheid van de data op Olympus en Delphi te waarborgen is gekozen voor:

- Opslag: Voor opslag maakt i2i gebruik van een high-performance striped RAID-5 DAS array met een schaalbare capaciteit van op dit moment 15 TB per server. Voor de bewaking van privacy gevoelige data wordt gebruik gemaakt van hardware level 128/256 bit AES encryptie.
- Netwerk: Om absolute veiligheid te waarborgen staan alle privacygevoelige gegevens op servers die geen netwerkverbinding tot het internet hebben, waarmee ongeautoriseerde toegang vrijwel uitgesloten is.

- Toegang en logging: Uitsluitend analisten hebben met een eigen login en password toegang tot Olympus en Delphi, waarbij alle toegang en transacties permanent gelogd worden.
- Backups: Wekelijks doet i2i backups met 256-bit encryptie die fysiek worden meegenomen naar een aparte veilige locatie.

Alle werkstations en laptops van de werknemers van i2i zijn voorzien van 256-bit encryptie van de gegevensdragers.

Voorts is het kantoor beveiligd met digitale toegangspasjes en een toegangscode, daarnaast is er in het gebouw 24h bewaking.

Compliance met wet en regelgeving

De verwerking van persoonsgegevens van zowel de verzekerden als de zorgverleners is in overeenstemming te zijn met de Wet Bescherming Persoonsgegevens, de Algemene Verordening Gegevensbescherming, de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen, het daarbij behorende Addendum Zorgverzekeraars en het Protocol materiële controle.

Verwerking persoonsgegevens verzekerden

Gegevens die tot de identificatie van een persoon zouden kunnen leiden worden door i2i geanonimiseerd door een combinatie van pseudonimisering en hashing; dat wil zeggen dat alleen versleuteld BSN, leeftijd, geslacht en postcode4 aangeleverd worden, zodat voor i2i niet herleidbaar is op welke individuen declaraties betrekking hebben maar individuen wel gevolgd kunnen worden tussen verschillende zorgverleners.

Risico-analyse privacy en herleidbaarheid van persoonsgegevens

i2i voert halfjaarlijks een risico-analyse uit op de aangeleverde data om te bepalen wat de risico's zijn met betrekking tot privacy en herleidbaarheid van gegevens. Deze risico-analyse vindt ook plaats bij nieuwe regelgeving met betrekking tot privacy, nieuwe dataformaten en nieuwe inzichten in de markt met betrekking tot privacy en herleidbaarheid.

i2i bepaalt op veldniveau van alle aanleveringen de risico's. De risico-analyse per data-element is op verzoek beschikbaar. In dit document is het volgende beschreven: 1) Standaardcode, recordnaam en naam gegevenselement volgens de desbetreffende standaardbeschrijving en functie van het gegevenselement; 2) Risico op directe herleidbaarheid; 3) Risico op indirecte herleidbaarheid; 4) Risico indirecte herleidbaarheid na maatregelen; 5) Overwegingen bij de risico-inschatting; 6) Genomen maatregelen.

Samenvatting van de gegevenselementen met hoog risico op herleidbaarheid en de genomen maatregelen:

Gegevenselementen	Voorbeelden	Maatregelen			
		Anonimiseren door combinatie van pseudonimisering	Anonimiseren door verwijderen	Anonimiseren door generalisatie en aggregatie	Anonimiseren door Generalisatie
BSN		X			
Verzekerde nummer		X			
Postcode				X	
Geboortejaar				X	
Namen en adressen	Naam_1_voorvoegsel, Naam_1_code, Naam_2, Naam_2_voorvoegsel, Naam_2_code, Voorletters, Huisnr, Huisnr_toevoeging in Dis-standaard		X		
Landcode					X
Patientnummer bij instelling			X		
Factuurnummer			X		

De volgende maatregelen zijn genomen op het niveau van data-elementen:

Anonimiseren door verwijderen van een gegevenselement

Het gegevenselement wordt onzichtbaar gemaakt door het te overschrijven met #. I2i kan de oorspronkelijke waarde niet achterhalen. Dit geldt voor de meeste persoonsgegevens. Alleen als het gegevenselement essentieel is voor benchmarking en een middel of laag risico vormt voor directe herleidbaarheid, wordt niet geanonimiseerd. In dat geval maakt i2i de noodzaak van niet verwijderen voor het uitvoeren van de doelstellingen aannemelijk.

Anonimiseren door middel van een combinatie van pseudonimisering en salted en keyed hashing van een gegevenselement

Deze vorm van anonimiseren vindt plaats als twee-staps proces, waarin twee keer wordt gehasht met behulp van een salted en keyed hash. De hashing van de tweede stap wordt bewaakt door de SBPDDDP. Op deze wijze kan de oorspronkelijke waarde van het gegevenselement door i2i niet meer worden achterhaald, maar de uniciteit van het gegevenselement blijft gehandhaafd. In deze gevallen maakt i2i de noodzaak van deze vorm van anonimiseren voor het uitvoeren van de doelstellingen aannemelijk. Dit geldt voor BSN en polisnummer van de verzekerde.

Anonimiseren door generalisatie van een gegevenselement

Het risico op identificatie van een persoon kan bij sommige gegevenselementen worden geminimaliseerd door het te beperken tot een niet significant deel van het gegevenselement. Dit passen wij toe bij postcode (alleen cijfers) en bij geboortedatum (alleen geboortejaar). Aangezien in

beide gevallen nog specifieke risico's bestaan worden ze hierna apart beschreven. Hiervoor passen we anonimiseren door aggregatie toe.

Postcode

i2i ontvangt alleen de 4 cijfers van de postcode (generalisatie). De letters van de postcode worden vervangen door #. In postcodes in dunbevolkte gebieden is dit niet voldoende. I2i wijzigt alle postcodes die niet aan de norm van minimaal 200 inwoners volgens het CBS voldoen, naar 0000 (aggregatie).

Geboortedatum

i2i ontvangt alleen het geboortejaar(generalisatie). Maand en dag van de geboortedatum worden vervangen door #. Het aantal verzekerden met een leeftijd van 100 jaar of ouder is zo laag, dat dit een risico op (in)directe herleidbaarheid geeft (aggregatie). i2i neemt de volgende maatregelen om te borgen dat de leeftijd van personen van 100 jaar of ouder niet achterhaald kan worden, ook niet indirect met behulp van oude aanleveringen:

- De leeftijd van verzekerden van 97 jaar en ouder wordt vastgeprikt op 97 op het moment van nu.
- In de aangeleverde bestanden wordt het geboortejaar gewijzigd voor de personen die 97 jaar of ouder zijn op het moment van anonimiseren
- In de data van i2i wordt ingebouwd dat dit geboortejaar wordt aangepast bij iedere jaarovergang.
- i2i vernietigt aangeleverde bestanden na 2 jaar.

Verwerking persoonsgegevens zorgverleners
De verwerking van de gegevens van zorgverleners is ook in overeenstemming met de Wet Bescherming Persoonsgegevens. De belangrijkste criteria zijn dat de verwerking van de persoonsgegevens noodzakelijk en proportioneel zijn. De zorgverleners waarvan de gegevens worden verwerkt vallen in twee categorieën uiteen. Van de eerste groep zorgverleners (geen DDD-partners) worden enkel de (declaratie)gegevens gebruikt in het kader van de risicoanalyse en de daarbij behorende benchmark. In het kader van de wettelijke controle taak van de verzekeraar is een dergelijke controle noodzakelijk en proportioneel. De tweede groep zorgverleners die deelnemen aan het DDD-project geven contractueel hun toestemming aan i2i om hun gegevens te verwerken en daarmee is de verwerking noodzakelijk en proportioneel.

Aanvullende maatregelen

Naast de bovenstaande infrastructurele maatregelen is er een aantal aanvullende maatregelen die i2i neemt om de veiligheid van data te waarborgen:

a) Auditor: Het staat verzekeraars en zorgverleners vrij om te allen tijde een auditor in te schakelen om vast te stellen of de daadwerkelijke omgang met data van derden bij i2i in overeenstemming is met het hier beschreven proces.
b) Bewerkersovereenkomst: Op verzoek kan i2i specifieke aanvullende bewerkersovereenkomsten met verzekeraars of zorgverleners sluiten.
c) Werknemers: alle werknemers van i2i hebben een geheimhoudingsverklaring getekend en mogen onder geen enkele voorwaarde ruwe data van zorgverleners meenemen buiten kantoor. De geheimhoudingsverklaringen zijn op verzoek in te zien.