Menzis informatiebeveiliging

Als zorgverzekeraar verwerkt Menzis veel gegevens waarvan het merendeel digitaal. Dit doet Menzis voor:
- ✓ Inkoop van zorg voor afsluiten en vastleggen van overeenkomsten met zorgverleners;
- ✓ Administratie van verzekerden voor het vastleggen polissen;
- ✓ Verwerken van declaraties voor vergoeden van zorgkosten;
- ✓ Verlenen van service voor de ondersteuning en het beantwoorden van vragen van verzekerden;
- ✓ Administratie van zorgaanvragen ingeval voor verkrijgen van zorg een machtiging noodzakelijk is;
- ✓ De incasso van premies en eigen bijdrages van verzekerden;

Daarnaast levert Menzis nog:
- ✓ Zakelijke vitaliteit en gezondheids diensten middels Menzis WerkGezond;
- ✓ Persoonlijke gezondheids en leefstijl ondersteuning via SamenGezond.nl;
- ✓ Administratie van de zorgkantoren (Wet Langdurige Zorg) in de regio's Groningen, Twente en Arnhem.

Ondersteunend daaraan zijn bedrijfsfuncties zoals: financiële administratie; Marketing & Sales; Actuariaat; Controle en fraudebeheersing; P&O, facilitaire zaken, IT, juridische zaken, en bedrijfsbureau.

Vanwege de hoge mate aan privacy gevoelige gegevens doet Menzis dit met de grootste zorgvuldigheid en met toepassing van een volledige set aan technische en organisatorische maatregelen.

Algemeen
Menzis voorziet zelf in de ondersteuning, beheer en beveiliging van de meeste en belangrijkste informatiesystemen. De beheerprocessen voorzien in technisch beheer, applicatieontwikkeling en -beheer, functioneel beheer, change- en releasemanagement, en incidentmanagement.
Daar waar gebruik gemaakt wordt van externe partijen maakt Menzis afspraken over dienstverlening, beveiliging en continuïteit in lijn met de Menzis standaarden. Menzis behoudt de verantwoordelijkheid en houdt controle op handhaven van de afgesproken maatregelen. Beoordeling van leveranciers op deze onderdelen is opgenomen in het controlesysteem van Menzis.

Beveiligingsmaatregelen
Menzis hanteert een informatiebeveiligingsbeleid dat is gebaseerd op de ISO27001 en beveiligingsmaatregelen gebaseerd op de ISO27002. Dit stelsel wordt gecontroleerd aan de hand van een op COBIT gebaseerd controleraamwerk. Hierop wordt toezicht gehouden door 2^{e} lijn controle teams, door de IT-auditors (RE) van de auditafdeling, door de externe accountant, en door NZA en DNB.
De belangrijkste maatregelen zijn:
- Systeembeveiliging door middel van hardening vastgelegd in platform security baselines, vulnerability en patchmanagement, en anti malware oplossingen;
- Maandelijkse security testing en review.
- Netwerkbeveiliging door middel van door firewalls gescheiden zones, gebruik van veilige protocollen, intrusion detection en prevention, content inspection, en malware en phishing preventie;
- Fysieke beveiligingsmaatregelen en toepassing van toegangspassen;
- Toepassen van secure software development standaarden;
- Gescheiden ontwikkel test acceptatie en productie omgevingen;
- Functiescheiding en logische toegangsbeveiliging;
- Privileged Access Management op verregaande bevoegdheden;
- Geheimhoudingsverklaring, achtergrondonderzoek, opleiding en awarenss training van personeel;
- Logging en securitymonitoring door middel van een SIEM oplossing en een 24/7 Security Operations Centre;

Informatieverwerking
De administratieve processen voor de zorgverzekering (polis, declaraties, debiteurenbeheer) worden afgehandeld in het softwarepakket Oracle Health Insurance hetgeen specifiek voor de Nederlandse zorgverzekering is gebouwd en wordt onderhouden. Dit pakket voorziet o.a. standaard in een koppelingen met Vecozo voor verwerking van zorgverlener declaraties.
Voor serviceverlening wordt gebruik gemaakt van de Salesforce Servicecloud waarin klantcontacten worden vastgelegd. Salesforce is o.a. ISO27001 gecertificeerd en data wordt binnen de Europese Privacy regels verwerkt. Salesforce maakt gebruik van onafhankelijk audit toezicht op haar dienstverlening en beveiliging. Menzis ziet daarop toe door beoordeling van de controle rapportages.

De zakelijke financiële administratie wordt in eigen beheer gevoerd ondersteund door online inkoop-, contract- en procuratie software. Ook deze dienst staat onder controle van onafhankelijk toezicht. Voor deze dienst zijn beveiliging en controle integraal onderdeel van de beheersmaatregelen van Menzis.

Document- en output management voorziet in verwerking van de papier en e-mail stromen en de archivering in het document management systeem. Drukwerk en postbehandeling zijn uitbesteed. Over privacybescherming zijn specifieke afspraken gemaakt waarover periodiek inspecties worden uitgevoerd.
Het systeem voor het document management is ingericht om toegang tot documenten te beperken tot de verschillende bedrijfsonderdelen en bedrijfsprocessen van Menzis.

Bedrijfsmatig wordt gebruik gemaakt van standaard (cloud) diensten zoals Microsoft Office365 en e-mail, en diensten voor HRM en gebouwbeheer. Ook deze voorzieningen worden door Menzis gecontroleerd en voldoen aan alle Menzis beveiligingsnormen. Veilig gebruik van de e-mail voorziening wordt mede gewaarborgd door richtlijnen in de gedragscode waarin onder andere het verbod op mailen van gevoelige persoonsgegevens is opgenomen. Dit wordt ondersteund door verplichte deelname aan de periodieke e-learning trainingen op het gebied van informatiebeveiliging, privacy en integriteit.

Continuïteit en technische beveiliging
Menzis beschikt over een dubbel uitgevoerde technische infrastructuur (netwerk, datacenter, storage, systemen) waarbij door middel van virtualisatie de 2 rekencentra elkaars functie kunnen overnemen. Replicatie van gegevens vindt doorlopend plaats zodat er geen gegevensverlies kan optreden.
Het interne netwerk is ingedeeld in meerdere gescheiden zones ten behoeve van werkplekken, applicaties, data en databases, en een DMZ zone voor internet- en externe verbindingen.
Voor toegang van buitenaf is multi factor authenticatie vereist. Mobiele apparaten zijn voorzien van beheersoftware die versleuteling en beveiligingsinstellingen controleert.
Voor alle externe verbindingen geldt dat door middel van proxy voorzieningen de interne systemen zijn afgeschermd. Voor uitwisseling van gegevens gebruikt Menzis een centraal beheerde sFTP oplossing, beveiligde webservices, of voor adhoc gebruik en veilig mailen, een gecertificeerde secure fileshare cloud dienst.