Nota informatieveiligheid en privacy

Synthese en vuistregels inzake de beveiliging van medische gegevens

(op basis van besprekingen binnen de subwerkgroep “medische gegevens”)

(NOTA MEDSEC)

INHOUDSOPGAVE

1. Inleiding

Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).

Dit document geeft de standpunten weer die de subwerkgroep "Medische gegevens" in neemt met betrekking tot de beveiliging van medische gegevens. Het is opgesteld met de bedoeling:

- de geneesheren een leidraad te overhandigen met betrekking tot de implementatie en de toepassing van veiligheidsmaatregelen voor medische gegevens, en
- de gesprekken met de informatieveiligheidsconsulenten en met de functionarissen voor de gegevensbescherming te kunnen aanknopen.

In het kader van de bescherming van de medische persoonsgegevens krijgt elke verantwoordelijke geneesheer op de eerste plaats een conceptuele opdracht mee, met name maken voor en het doorspelen van veiligheidsinstructies (het vastleggen van veiligheidsdoelstellingen en het bepalen en de voortdurende bijwerking van het beoogde veiligheidsniveau) aan de informatieveiligheidsconsulent en aan de functionaris voor de gegevensbescherming en het onderhoud van de instructies op de tijdstippen dat de noodzaak zich hiertoe voordoet. In het bijzonder heeft elke verantwoordelijke geneesheer de opdracht om de specifieke veiligheidsproblemen van zijn/haar organisatie te bestuderen met de informatieveiligheidsconsulent en met de functionaris voor de gegevensbescherming ten einde in functie van de situatie passende maatregelen uit te werken[1]. De aard en de omvang van deze maatregelen kunnen verschillend zijn in elke organisatie en hangen van vele factoren af, zoals:

- de financiële slagkracht van de organisatie;
- de mogelijkheid om binnen de organisatie veranderingen door te voeren en de snelheid waarmee dit kan gebeuren;

Van een organisatie kan echter niet gevraagd worden, zonder verwijl, zware inspanningen te leveren[2]. Het gelijkmatig spreiden van de inspanningen over een aanvaardbare tijdsspanne zal betere resultaten afwerpen. De geleverde inspanningen moeten in evenredigheid zijn met het belang van de medische gegevens waarop deze betrekking hebben. In de mate van het mogelijke is het te vermijden dat een organisatie procedures en werkwijze grondig moet aanpassen of dat bestaande administratieve structuren onnodig worden verzwaard. Het moet wel de ambitie zijn om het informatieveiligheidsniveau elk jaar merkbaar te verbeteren.

Daar waar de verantwoordelijke geneesheer vooreerst een conceptuele missie heeft, staat de informatieveiligheidsconsulent en de functionaris voor gegevensbescherming, inzake de beveiliging van medische persoonsgegevens, in voor de opvolging met betrekking tot de correcte invoering van de instructies die hij/zij van de verantwoordelijke geneesheer mocht ontvangen. Het toezicht op de invoering van de instructies behoort toe aan de verantwoordelijke geneesheer.

[1] Een verantwoordelijke arts kan aan de subwerkgroep "Medische gegevens" altijd een advies vragen met betrekking tot het feit of de ingevoerde of voorgestelde informatieveiligheidsmaatregelen voldoende zijn.

[2] De kosten die met de bescherming van medische gegevens gepaard gaan, moeten ingeschreven worden op het informatieveiligheidsbudget dat elke organisatie dient op te stellen in het kader van artikel 7 van het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de openbare instellingen van sociale zekerheid (OISZ).

2. Standpunten inzake de beveiliging van medische gegevens

2.1 Medische gegevens

2.1.1 Definitie

De subwerkgroep "Medische gegevens" sluit zich aan bij de redenering van het Toezichtscomité[3] bij de bepaling van een definitie van de term "Medisch gegeven". Deze redenering leidt tot de conclusie dat zowel de context (doelmatigheidsbeginsel) waarbinnen een gegeven gebruikt wordt als de aard van een gegeven bepalend is of een gegeven als medisch of als niet medisch moet beschouwd worden[4].

De redenering van het Toezichtscomité is op de volgende twee principes gebaseerd:

- teleologische interpretatie: in dit kader dient een begrip uitgelegd te worden in functie van het doel waarvoor het werd gedefinieerd. In eerste instantie dienen dus de te bereiken doelen te worden bepaald en vervolgens dient het begrip "medisch gegeven" op basis van deze doeleinden te worden geïnterpreteerd.

  De motieven die de wetgever ertoe hebben aangezet de verwerking van bepaalde gegevens onder het toezicht van een geneesheer te plaatsen zijn dat, de tussenkomst van een geneesheer, voor sommige gegevens, in het kader van de bescherming van de persoonlijke levenssfeer, een toegevoegde waarde biedt. Voor de gegevens waar deze tussenkomst evenwel geen toegevoegde waarde betekent, schijnt deze tussenkomst geen vereiste te zijn.

  Een voorbeeld ter illustratie: voor de verwerking van een adres is de tussenkomst van een geneesheer niet noodzakelijk aangezien iedereen de inhoud ervan correct kan interpreteren. Een adres is dus geen medisch gegeven. Bovendien wordt, door het plaatsen van een adres onder het toezicht van een geneesheer, de informatieveiligheid of privacy ervan niet groter. Een diagnose of een nomenclatuurcode daarentegen kan alleen correct geïnterpreteerd worden door een geneesheer. Dit is dus wel een medisch gegeven.

- eenduidig: ofwel wordt een gegeven steeds als medisch beschouwd ofwel nooit. Een tussenweg is niet aanwezig. Het is immers niet werkbaar te beweren dat een adres in 99% van de gevallen geen medisch gegeven is en in 1% van de gevallen, de uitzondering, wel een medisch gegeven is (bijvoorbeeld omdat een verblijf in een psychiatrische instelling eruit afleidbaar is[5]). Dit zou immers betekenen dat het gegeven "adres", indien opgenomen in een gegevensbank, onder het toezicht van een geneesheer zou moeten worden geplaatst. Hierdoor zullen bijna alle bestanden onder de controle van een geneesheer komen te vallen. Een andere oplossing, met name het groeperen van deze adressen in een afzonderlijk bestand blijkt ook niet ideaal aangezien iedereen hieruit onmiddellijk zou kunnen besluiten dat het betrokken bestand vertrouwelijke gegevens bevat.

Het aantal medische gegevens kan het best zoveel mogelijk beperkt blijven. Teveel gegevens als medisch klasseren kan immers nadelige gevolgen hebben voor de bescherming van de echte medische gegevens.

---

[3] Het Toezichtscomité definieerde de term "Medisch gegeven" in haar activiteitenverslag van 1992 (blz. 34, 35). De heer Frank Robben verduidelijkte de redenering van het Toezichtscomité met betrekking tot de definitie van het begrip "Medisch gegeven" in zijn nota van 19 mei 1995 voor de leden van de subwerkgroep "Medische gegevens" met als referentie A1/U03/95/150.pu.

[4] De subwerkgroep "Medische gegevens" verklaart niet te geloven in een definitie maar wel in de redenering die tot een definitie leidt. Een definitie voorstellen die altijd geldig is lijkt een quasi onmogelijke opdracht. De subwerkgroep zet zich met dit standpunt expliciet af tegen diegenen die van mening zijn dat enkel de aard van een gegeven, en dus niet de context waarin het verwerkt wordt, van doorslaggevende betekenis is om als medisch of als niet medisch bestempeld te worden. Deze zienswijze verzaakt immers aan een basisbeginsel inzake de bescherming van de persoonlijke levenssfeer, met name het doelmatigheidsbeginsel. Het miskennen van deze fundamentele doelstelling impliceert dat zowat alle gegevens medisch zijn en de verwerking ervan als dusdanig onder het toezicht en de verantwoordelijkheid van een geneesheer dient te geschieden. De tussenkomst van een geneesheer zal, indien hij/zij verantwoordelijk wordt gesteld voor de verwerking van quasi alle gegevens, uiteindelijk een maat voor niets zijn aangezien de aandacht van de geneesheer met betrekking tot de bescherming van medische gegevens hierdoor aanzienlijk zal afnemen.

[5] Een bestand met enkel adressen van personen die in een psychiatrische instelling verblijven zijn wel als medische gegevens te beschouwen.

De geneesheer bepaalt zelf, in functie van de omstandigheden, en binnen zijn/haar organisatie, wat wel en wat niet een medisch gegeven is. De beoordeling of een gegeven medisch is of niet en met andere woorden een bijkomende bescherming dient te genieten, moet overgelaten worden aan de geneesheer die in dit kader over de nodige appreciatiebevoegdheid moet beschikken. Het aan banden leggen van deze appreciatiebevoegdheid, door het uitwerken van precieze definities, is dan ook te vermijden.

2.1.2 Medische gegevens in de strikte zin en administratief medische gegevens

De subwerkgroep "Medische gegevens" aanvaardt het principe om medische gegevens in verschillende categorieën onder te verdelen[6] om zodoende verschillende beschermingsniveaus te kunnen invoeren. Zo is het mogelijk te spreken over medische gegevens in de strikte zin en administratief medische gegevens[7]. De beslissing tot het opdelen van medische gegevens in verschillende klassen berust bij elke instelling afzonderlijk. Het is immers onbegonnen werk om in dit vlak algemeen geldende spelregels en richtlijnen vast te leggen.

De creatie van verschillende medische gegevenscategorieën laat toe een onderscheid te maken tussen verschillende types van medisch bevoegden. Bijvoorbeeld:

- de personen met een algemene medische bevoegdheid: krijgen toegang tot alle medische gegevens en mogen alle medische gegevens verwerken;
- de personen met een specifieke medische bevoegdheid: krijgen enkel toegang tot bepaalde medische gegevens en mogen enkel specifieke medische gegevens verwerken.

2.1.3 Toegang tot medische gegevens

De aanduiding van de personen die betrokken zijn bij de verwerking van medische persoonsgegevens of die er toegang toe hebben moet nominatief gebeuren. Deze aanduiding kan gebeuren onder verwijzing naar functies, op voorwaarde dat de functies voldoende nauwkeurig beschreven zijn en duidelijk vastgesteld is welke individuele personen welke functie uitoefenen[8].

Per functie moeten dan de inhoud en de draagwijdte van de toegangsmachtigingen duidelijk worden vastgelegd[9]. Het vastleggen van deze machtigingen dient te gebeuren op basis van het doelmatigheidsbeginsel. Concreet kunnen deze toegangsmachtigingen bijvoorbeeld beschreven worden aan de hand van autorisatietabellen, die per soort van basisverwerking (raadplegen, toevoegen, wijzigen, verwijderen) aangeven wie ze mag uitvoeren.

De invoering van het principe van de functiebeschrijving treft een regeling met betrekking tot de vragen wie toegang heeft tot medische gegevens en tot hoever deze toegang reikt. Zo kunnen de hiernavolgende personeelscategorieën toegang hebben tot medische gegevens op voorwaarde dat deze toegang opgenomen werd in de betrokken functiebeschrijving: het invoeren van medische besluiten door niet-medisch personeel, de ronddeling van medische briefwisseling door niet-medisch personeel, de behandeling van medische dossiers door niet-medisch personeel, ...

---

[6] Een praktische oefening gebeurde reeds door Fedris en is terug te vinden in de technische nota 94/3 met betrekking tot de samenstelling van het medisch dossier.

[7] Het maken van een onderscheid tussen administratief medische gegevens en strikt medische gegevens is niet altijd even gemakkelijk. Bepaalde administratief medische gegevens worden immers medische gegevens wanneer deze gecombineerd worden met andere gegevens. Bij informatisering blijkt de onderlinge combinatie van gegevens gemakkelijk te verwezenlijken (bijvoorbeeld bij data analytics). Deze elementen zijn dan ook niet uit het oog te verliezen bij het opdelen van medische gegevens in categorieën.

[8] Hierbij zou het geen slechte zaak zijn, mochten organisaties elementaire functiebeschrijvingen uitwerken voor ten minste de medische functies (verantwoordelijke arts inbegrepen). De beste manier om dit aan te pakken is de personeelsleden zelf een beschrijving van hun functie te laten maken en deze later te laten stroomlijnen door de personeelsdienst.

[9] In het kader van de toekenning van toegangsautorisaties tot medische gegevens aan de personeelsleden dient gevraagd te worden welke medische gegevens zij nodig hebben voor de uitoefening van hun functie. Het zijn immers zij die het best geplaatst zijn om te bepalen welke gegevens zij nodig hebben. De gevraagde toegangsautorisaties moeten achteraf wel, per persoon en door de verantwoordelijke geneesheer, op hun noodzaak geëvalueerd worden ten einde misbruiken te voorkomen.

GEBRUIKERSGROEP X				
Gegevensomschrijving	Toevoegen (add / write)	Raadplegen (read / consult)	Wijzigen (change / modify)	Verwijderen (delete / erase)
Gegeven a	X	X		X
Gegeven b	X		X	
Gegeven c	X	X	X	X
…				

De toekenning van toegangsmachtigingen met betrekking tot papieren documenten kan volgens dezelfde principes gebeuren als de toekenning van autorisaties met betrekking tot elektronische gegevens. Het volstaat in dit geval namelijk om de gegevens a, b, c te vervangen door formulieren en de mogelijk uit te voeren handelingen eventueel aan te passen.

Het is de taak van de informatieveiligheidsconsulent en de functionaris voor gegevensbescherming erop toe te zien of de personeelsleden zich houden aan de autorisaties zoals deze vermeld staan in hun functiebeschrijving.

2.1.4 Uitwisseling van medische gegevens tussen verschillende interne diensten (zoals boekhouding, juridische dienst, dienst geschillen)

De vraagstelling wie medische gegevens mag uitwisselen, is uitgebreid aan bod gekomen in de paragraaf 2.1.3. ("Toegang tot medische gegevens"). De vraagstelling welke gegevens er voor uitwisseling in aanmerking komen, is het de geneesheer die zal oordelen wat er mag doorgegeven worden en wat niet. De geneesheer moet hierbij wel de geldende wetgeving terzake volgen.

2.1.5 Uitbesteding van opdrachten met betrekking tot de verwerking van medische gegevens

Voor organisaties die in onderaanneming / in opdracht werken gelden dezelfde informatieveiligheidsmaatregelen als deze die voor de opdrachtgevende organisatie van toepassing zijn. Het veiligst is om deze aspecten duidelijk contractueel te voorzien en expliciet rekening te houden met de volledige levenscyclus van de informatie (vanaf de creatie tot en met de archivering of verwijdering). De opdrachtgever heeft tot taak erop toe te zien dat de onderaannemer de informatieveiligheidsregels respecteert. De eventuele aanstelling van een geneesheer bij de onderaannemer, indien deze in opdracht van de uitbestedende organisatie, medische persoonsgegevens verwerkt, geniet bij voorkeur een contractuele oplossing.

2.2 Medisch dossier[10]

2.2.1 Administratief medisch dossier en medisch dossier met louter medische stukken

Elke organisatie neemt de beslissing of zij wenst over te gaan tot de creatie van een administratief medisch dossier en een medisch dossier met louter medische stukken. Een dossier met zowel administratief medische stukken als medische stukken moet een beveiliging genieten alsof het enkel medische stukken zou bevatten (dus de strengst mogelijke beveiliging). Een dossier met enkel administratief medische stukken is minder streng te beveiligen. Het vermengen van een medisch dossier met een administratief medisch dossier heeft als nadeel dat een dossier niet afzonderlijk verkrijgbaar is waardoor het langer geïmmobiliseerd wordt.

[10] Een geneesheer moet opletten welke gegevens hij in een medisch dossier optekent. Niet relevante gegevens of gegevens die geen toegevoegde waarde hebben voor het medisch dossier mogen niet worden neergeschreven.

2.2.2 Een sociaal verzekerde beschikt binnen een organisatie over verschillende medische dossiers (geen gebruik van een uniek identificatie nummer)

Een oplossing voor dit probleem kan in de eerste plaats gezocht worden in organisatorische maatregelen die kunnen verschillen per organisatie, door te informatiseren en door het gebruik van het Rijksregisternummer te verplichten. Eén mogelijke oplossing is een uniek medisch dossier aan te leggen kan zijn per individu. Deze werkwijze biedt een aantal voordelen waarvan de belangrijkste zijn:

- vereenvoudigd dossierbeheer;
- concentratie van informatie waardoor alle gegevens terug te vinden zijn in één dossier en tegenstrijdige beslissingen kunnen vermeden worden. Door deze concentratie kan er eveneens een verbetering in het beslissingsproces optreden.

Elk dossier moet gemakkelijk te lokaliseren zijn[11] en nieuw binnenkomende documenten/stukken met betrekking tot een bepaald persoon moeten steeds kunnen gekoppeld worden aan de reeds bestaande gegevens van die persoon.

Het aan elkaar koppelen van verschillende dossiers van dezelfde persoon kan elektronisch gebeuren zodat de opvrager van een dossier verwittigd wordt indien er voor dezelfde persoon nog andere dossiers bestaan.

2.2.3 Circulatie van medische dossiers

Dit probleem kan opgelost worden door het nemen van gepaste organisatorische maatregelen (bijvoorbeeld door het plaatsen van papieren medische dossiers in een briefomslag die vervolgens dichtgeniet en geparafeerd wordt).

Sensibilisering van het personeel omtrent medische dossiers is essentieel. Het personeel aansporen om dossiers/documenten/stukken die niet voor hen bestemd zijn, met inachtneming van de algemene beginselen van het briefgeheim, onmiddellijk terug te sturen naar de afzender of direct door te sturen naar de rechtmatige bestemmeling (indien deze bekend is binnen de organisatie).

2.2.4 Kwalificaties van medisch personeel die medische dossiers behandelen/beheren

Dit kan eenvoudig opgelost worden door in de functiebeschrijving het beoogde profiel te laten opnemen. Zo kan een geneesheer bepaalde eisen stellen inzake de vaardigheden, de scholingsgraad en de ervaring waarover een kandidaat dient te beschikken om medische dossiers te behandelen/beheren.

Bij de aanwerving of de vervanging van personeelsleden dient de personeelsdienst rekening te houden met de gestelde eisen. De klassering van medische dossiers bijvoorbeeld vereist dat de persoon in kwestie de nodige nauwkeurigheid en discipline aan de dag legt bij de uitvoering van dit werk, eigenschappen die niet aan iedereen gegeven zijn.

2.2.5 Fysische toegang tot het medisch archief (medische dossiers) en de installatie van een afzonderlijk archief voor medische dossiers

2.2.5.1 Fysische toegang tot medische dossiers en het medisch archief

De uitwerking van de nodige maatregelen moet gebeuren in samenwerking met de veiligheidsconsulent. De na te streven doelstelling is evenwel dat enkel medisch bevoegden toegang krijgen tot medische dossiers.

[11] Gemakkelijke lokalisatie kan opgevangen worden door middel van de invoering van een geïnformatiseerd dossierbeheer. Dit laat immers toe om op gelijk welk moment te achterhalen waar een medisch dossier zich precies bevindt.

De te implementeren veiligheidsmaatregelen moeten afhangen van de risico's die zich kunnen voordoen (zoals de toegangsmaatregelen tot een archief waar medische dossiers gemakkelijk terug te vinden zijn, zijn verschillend van de toegangsmaatregelen voor lokalen waar medische dossiers zich op de bureaus bevinden). Iedere organisatie is verschillend en elkeen moet in functie van zijn specifieke situatie maatregelen treffen. Het is hierbij noodzakelijk een afweging te maken tussen informatieveiligheid en efficiëntie[12].

De toegang tot de lokalen waar het mogelijk is de lokalisatie van een bepaald medisch dossier terug te vinden, moet eveneens beveiligd zijn. Enkel personen die toegang hebben tot medische dossiers mogen weten waar een medisch dossier zich bevindt.

2.2.5.2 Afzonderlijk archief voor medische dossiers

Het gecentraliseerd en apart opslaan van medische dossiers is aan te raden daar het op zijn minst twee niet te versmaden voordelen met zich meebrengt:

- dossiers zijn gemakkelijk terug te vinden;
- toegang is beter beheersbaar;

Indien een organisatie geen afzonderlijke archiefruimte aanlegt voor medische dossiers, dan mag dit op voorwaarde dat de organisatie er zorg voor draagt dat de toegang tot het archief goed is afgesloten en beperkt blijft tot de medisch bevoegden. Het opslaan van papieren medische dossiers op digitale informatiedragers is ook een mogelijke oplossing (zie bewijskracht[13]).

2.2.6 Logische toegang tot medische dossiers

Een oplossing voor dit probleem moet gezocht worden in functie van de specifieke situatie van de organisatie en in overleg met de informatieveiligheidsconsulent en de functionaris voor gegevensbescherming. Meestal is een programmatorische aanpassing voldoende.

2.3 Toegang tot het gebouw en lokalen

De toegang tot de lokalen en tot het gebouw is geen specifiek medisch probleem maar een algemeen informatieveiligheidsprobleem. De oplossing moet komen van de informatieveiligheidsconsulenten. Wel dient de verantwoordelijke geneesheer de eventuele problemen met de informatieveiligheidsconsulent te bespreken.

Medische vergaderingen[14] worden zowel tijdens als buiten de normale werkuren in niet geïsoleerde ruimtes gehouden: de meest aangewezen oplossing bestaat uit het treffen van geschikte organisatorische maatregelen eventueel in combinatie met technische maatregelen. De uitwerking van de nodige maatregelen moet gebeuren in samenwerking met de informatieveiligheidsconsulent.

[12] De leden van de werkgroepen "Informatieveiligheid" en "Medische gegevens" nemen het standpunt in dat, gelet op het belang van medische gegevens en de daarmee verbonden risico's, de (actieve en gearchiveerde) medische dossiers ook fysisch moeten worden beveiligd. De middelen (zoals kast, bureau, afgesloten lokaal) zijn door de organisatie zelf vast te leggen.

[13] Wet van 24 februari 2003 betreffende de modernisering van het beheer van de sociale zekerheid en betreffende de elektronische communicatie tussen ondernemingen en de federale overheid. Koninklijk besluit van 7 december 2016.

[14] Een medische vergadering is een vergadering waar medische dossiers worden besproken.

3. Veiligheidstechnieken

3.1 Authenticatie technieken

Er zijn verschillende vormen van authenticatie die eventueel gecombineerd kunnen worden om een hoger of lager niveau van beveiliging op te leveren. Daarbij zijn drie vormen van bewijs bruikbaar:

1. Iets dat je weet = Kennis

   Iets wat je weet is bijvoorbeeld een wachtwoord, een pincode of een geheime zin. Het is de bedoeling dat dit bewijs geheim is, het mag niet uitlekken om diefstal van de identiteit tegen te gaan. Een hacker zal proberen de identiteit van iemand over te nemen door een wachtwoord te raden, te achterhalen met behulp van bijvoorbeeld een keylogger[15]. Om die reden wordt in organisaties met medische gegevens dan ook het gebruik van lange wachtwoorden[16] afgedwongen die periodiek gewijzigd moeten worden. Als het goed is, zal de kraaktijd van een wachtwoord langer moeten zijn dan de vervaltermijn van de medische gegevens.

2. Iets dat je bezit

   Dit betekent dat het bewijs van de identiteit wordt geleverd door het gebruikmaken van een fysiek herkenningsteken dat door of namens het autoriserende systeem werd uitgereikt. Voorbeelden zijn tokens of een smartcard of een USB-sleutel. Hierbij wordt gebruikgemaakt van de vraag-antwoordfunctie: het autoriserende systeem stelt een vraag en degene die toegang vraagt, moet met behulp van het token een passend antwoord geven. Het grote voordeel van deze techniek is dat een persoon, die zich wenst aan te loggen, zowel over een geheime code als over een token moet beschikken en dat het berekende paswoord bij elke logon-beurt wijzigt.

3. Iets wat je bent = Persoonlijke eigenschap

   Een uniek identificerend kenmerk van een persoon wordt opgeslagen in een authenticatiedatabase[17]. Dit zijn de zogenaamde biometrische systemen die de persoonlijke karakteristieken of de gedragingen van een gebruiker trachten te herkennen. Gebruikte technieken zijn herkenning van de handtekening, vorm van de hand, vingerafdrukken, stemherkenning, gezichtsherkenning, netvlies/iris-scanners, enz. De nadelen die aan deze technieken verbonden zijn

   - niet altijd aanvaard door de gebruikers;
   - vrij duur;
   - niet altijd even betrouwbaar.

4. Geautomatiseerde authenticatie

   Computers en systemen maken gebruik van andere vormen van authenticatie. Ook kan gebruik worden gemaakt van een vorm van een Public Key Infrastructure (PKI), waarbij certificaten worden gebruikt. Bekende implementaties zijn 802.1X en SAML[18].

De organisaties dienen de nodige procedures te ontwikkelen voor het geval een gebruiker zijn/haar token niet terugvindt (diefstal, verlies). De manier waarop de toekenning van nieuwe tokens kan plaatsvinden, dient eveneens geregeld te worden. De authenticatietechnieken mogen enkel gebruikt worden voor het doel waarvoor ze werden

[15] Een keylogger is een programma of een stuk hardware waarmee men de toetsaanslagen tot zelfs de muisbewegingen van een computergebruiker kan registreren.

[16] Een degelijk lang wachtwoord is minimaal 12 karakters lang. Voor het testen van de degelijkheid van een wachtwoord kan iedereen terecht op https://www.safeonweb.be/nl/wachtwoordtest

[17] Dit wordt ook wel biometrie genoemd, het vaststellen van meetbare eigenschappen van mensen.

[18] Security Assertion Markup Language is een standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen. SAML biedt een XML-gebaseerd raamwerk voor het creëren en uitwisselen van beveiligingsinformatie van online partners. SAML wordt onderhouden door een internetgemeenschap en wordt publiekelijk bijgewerkt. Geïnteresseerden worden aangemoedigd om een bijdrage aan de ontwikkeling ervan te leveren.

geïmplementeerd en niet bijvoorbeeld voor het controleren van de tijdstippen waarop een gebruiker aanwezig is. De keuze van de authenticatietechniek kan verschillen per organisatie en dient overgelaten te worden aan de informatieveiligheidsconsulent in samenspraak met de functionaris voor gegevensbescherming.

3.2 Versleuteling technieken

Hiervoor verwijzen we naar beleidslijn “versleutelen” (BLD CRYPT) voor meer informatie.

3.3 Functiescheiding

Dit principe komt hier op neer dat binnen een organisatie geen enkel individu over de exclusieve bevoegdheid mag beschikken zodanig dat hij/zij de verwerking van een bepaalde transactie of een groep van transacties volledig beheerst. Dus een bepaalde verantwoordelijkheid wordt over meer dan één persoon gespreid. Deze opsplitsing wordt als interne controle doorgevoerd om fouten en misbruiken te vermijden/voorkomen. Het risico dat mensen samenwerken om deze interne controle te omzeilen wordt collusie genoemd.

Idealiter worden scheidingen aangebracht tussen besluitvorming/autorisatie, uitvoering, controle/bescherming, registratie en bewaring van medische gegevens zonder dat dit de efficiëntie al te zeer ondermijnt.

Een middel om de scheidingen in processen uit te tekenen is de functiescheidingsmatrix. In een dergelijk document wordt per proces aangegeven welke persoon (in welke functie) beschikkend, bewarend, registrerend, controlerend en uitvoerend is.

Ten einde het principe van functiescheiding praktisch toe te lichten, kan als voorbeeld de manier genomen worden waarop nieuwe toepassingen ontwikkeld worden in een geautomatiseerde informatie-verwerkende omgeving. Elke nieuw te ontwikkelen toepassing moet verschillende ontwikkelingsfases doorlopen. De belangrijkste fases zijn:

- de analysefase;
- de programmatiefase;
- de testfase;
- de fase waarbij het uitgetest programma in productie geplaatst wordt.

Zo wordt vermeden dat de persoon die een toepassing in productie plaatst dezelfde persoon is als de persoon die de toepassing heeft geschreven.

In de omgang met medische dossiers dient het principe van functiescheiding ingevoerd te worden. Het is in kleinere en middelgrote organisaties vrijwel onmogelijk om alle stappen in het proces perfect te scheiden. Daarom is het zaak om op een slimme manier functiescheidingen aan te brengen. In een gesprek met de controlerende instantie zal een goede afweging moeten worden gemaakt.

3.4 Beveiliging van medische gegevens op magnetische dragers

De belangrijkste problemen die zich voordoen m.b.t. medische gegevens op magnetische informatiedragers zijn de volgende:

- vertrouwelijkheidsprobleem: dit is eenvoudig op te lossen door de gegevens te vercijferen;
- transport van magnetische informatiedragers:
    - de informatiedragers moeten in een aangepaste container verzonden worden (zoals USB sleutel in een speciale belletjesomslag, magneetbanden en cassettes in een verzegelde koffer);
    - de verzender moet bij de verzending steeds zorgen dat er een bewijsmiddel van verzending is;
    - de informatiedragers moeten vergezeld worden van een verzendingsformulier waar minimaal volgende gegevens dienen vermeld te worden: naam en adres van de verzender, naam en adres van de bestemmeling en inhoud van de informatiedrager.

4. Vuistregels inzake de beveiliging van medische gegevens

1. De verantwoordelijke geneesheer laat zich bij de uitvoering van zijn informatieveiligheidsopdracht leiden door:

- de minimale normen informatieveiligheid en privacy die moeten worden nageleefd door de openbare instellingen van de sociale zekerheid (OISZ) met het oog op hun aansluiting op het netwerk van de Kruispuntbank van de sociale zekerheid (KSZ);
- de beleidslijnen op het niveau van de organisaties die deel uitmaken van het netwerk dat wordt beheerd door de Kruispuntbank van de sociale zekerheid (KSZ);
- het handboek "Informatieveiligheid Sociale Zekerheid";
- de medische gedragscode inzake de mededeling van medische gegevens van persoonlijke aard aan de gerechtigden op sociale zekerheid.

2. In het kader van de bescherming van de medische gegevens worden de taken tussen de verantwoordelijke geneesheer en de veiligheidsconsulent als volgt verdeeld:

- de belangrijkste opdracht van de verantwoordelijke geneesheer situeert zich op het conceptuele vlak, met name het formuleren van geschikte informatieveiligheidsdoelstellingen en de bepaling en de permanente bijsturing (in functie van de ontwikkelingen die een organisatie doormaakt en van de opgedane ervaring) van het beoogde informatieveiligheidsniveau (eventueel in samenwerking met de informatieveiligheidsconsulent en de functionaris voor gegevensbescherming). Het is ook de verantwoordelijke geneesheer die de informatieveiligheidsconsulent, de functionaris voor gegevensbescherming en de persoon die verantwoordelijk is voor het dagelijks beheer van de organisatie moet wijzen op de aanwezigheid van relevante risico's met betrekking tot de verwerking van medische persoonsgegevens;
- de informatieveiligheidsconsulent en de functionaris voor gegevensbescherming werken op basis van de door de verantwoordelijke geneesheer geformuleerde informatieveiligheidsdoelstellingen en het te bereiken informatieveiligheidsniveau aangepaste maatregelen uit. De uitwerking van deze maatregelen geschiedt bij voorkeur in samenwerking met de verantwoordelijke geneesheer. Benevens de uitwerking van maatregelen staan de informatieveiligheidsconsulent en de functionaris voor gegevensbescherming ook in voor de opvolging van de correcte en tijdige invoering[19] (samen met de verantwoordelijke voor het dagelijks bestuur die alvorens de invoering ervan zijn goedkeuring moet verlenen omtrent de voorgestelde maatregelen) en breiden informatieveiligheidsconsulent en de functionaris voor gegevensbescherming het veiligheidsplan en -budget uit met de maatregelen die betrekking hebben op de veiligheid van medische gegevens. Tot slot zorgen de informatieveiligheidsconsulent en de functionaris voor gegevensbescherming voor de nodige coördinatie met de verantwoordelijke geneesheer. Deze coördinerende rol heeft tot doel om te voorkomen dat de verantwoordelijke voor het dagelijks bestuur voor een welbepaald informatieveiligheidsprobleem twee uiteenlopende adviezen zou ontvangen (een dergelijke situatie is zoveel mogelijk te vermijden en mag zich slechts voordoen in het geval dat de informatieveiligheidsconsulent, de functionaris voor gegevensbescherming en de verantwoordelijke geneesheer een fundamenteel meningsverschil hebben over het geconstateerde probleem);
- naast een conceptuele opdracht is er voor de verantwoordelijke geneesheer ook een controlerende rol weggelegd. Deze bestaat erin toe te zien of de uitgewerkte informatieveiligheidsmaatregelen werden ingevoerd en in overeenstemming zijn met de door hem/haar geformuleerde doelstellingen;

3. De verantwoordelijke geneesheer werkt, in samenspraak met de informatieveiligheidsconsulent en de functionaris voor gegevensbescherming en rekening houdend met de specifieke situatie, geschikte organisatorische, technische en communicatieve maatregelen uit. De informatieveiligheidsconsulent en de functionaris voor gegevensbescherming behoren de maatregelen en de hiermee verband houdende kosten respectievelijk in te schrijven op het informatieveiligheidsplan en -budget (art. 7 van het koninklijk besluit van 12 augustus 1993 houdende de organisatie

[19] Niettegenstaande het feit dat de informatieveiligheidsconsulent en de functionaris voor gegevensbescherming in wezen geen uitvoerende rol hebben, is het niet uitgesloten dat ze zelf taken/activiteiten uitvoeren of verwezenlijken. Dit kan gebeuren op eigen initiatief of op vraag van de verantwoordelijke voor het dagelijks bestuur. Uiteraard spelen de organisatiestructuur van een organisatie en de specifieke situatie hierbij een cruciale factor.

van de informatieveiligheid bij de openbare instellingen van sociale zekerheid). De uiteindelijke beslissing omtrent de invoering van de uitgewerkte maatregelen berust bij de verantwoordelijke voor het dagelijks bestuur van de organisatie.

4. De aanduiding van de personen die betrokken zijn bij de verwerking van medische gegevens of die er toegang toe hebben moet nominatief gebeuren, volgens art. 26 van de Kruispuntbankwet. Deze aanduiding kan evenwel gebeuren onder verwijzing naar functies, op voorwaarde dat de functies voldoende nauwkeurig beschreven zijn en duidelijk vastgesteld is welke individuele personen welke functie uitoefenen. Praktisch gezien kan dit geïmplementeerd worden door de uitwerking en de invoering van functiebeschrijvingen. Een functiebeschrijving omvat onder andere de volgende elementen:

- een precieze omschrijving van de uit te voeren taken;
- de inhoud en de draagwijdte van de toegangsmachtigingen;
- de vermelding van de kwalificaties;
- ...

Zo kan elk personeelslid gemachtigd worden medische gegevens te verwerken op voorwaarde dat deze machtiging en de aard ervan in de functiebeschrijving van de betrokken persoon opgenomen staat.

5. De beslissing tot de creatie van verschillende medische gegevenscategorieën berust bij elke organisatie evenals de beslissing tot de creatie van verschillende categorieën van medisch bevoegden.

6. De ervaring leert dat medische dossiers niet altijd even snel worden geautomatiseerd als administratieve dossiers. In vele organisaties wordt er nog veel papier gebruikt voor de opslag van medische gegevens. Wanneer evenwel blijkt dat de opslag van medische dossiers onder elektronische vorm een informatieveiligheidsvoordeel biedt, dan moet worden aangedrongen op een versnelde informatisering. Aspecten die zeker een rol spelen bij de te maken keuze zijn onder andere de stand van de techniek, de beschikbare informatica- en informatieveiligheidskennis binnen een organisatie en de te leveren inspanningen (kosten/baten analyse)

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
1996		V1	Eerste versie	02/12/1996	02/12/1996
2017		V2017	Aanpassingen in het kader van de EU GDPR	14/07/2017	14/07/2017

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen uw contactinformatie door te geven aan de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO) van de organisatie.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Minimale Normen Definities informatieveiligheid en privacy”.

Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:

1. De Europese verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens van 27 april 2016[20];

De meeste openbare instellingen van sociale zekerheid vallen onder het toepassingsgebied van deze wet. Binnen elke openbare instelling van sociale zekerheid gebeurt de behandeling, de uitwisseling en de bewaring van medische gegevens van persoonlijke aard onder het toezicht en de verantwoordelijkheid van een arts. Deze artsen zijn ook nog gebonden door artikel 458 van het Belgische Strafwetboek (medisch beroepsgeheim) en door de Code van geneeskundige plichtenleer (Orde van geneesheren).

[20] http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&qid=1484310282035&from=NL

Bijlage C: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

ISO-norm 27002:2013	
Veiligheidsbeleid	
Organisatie van de informatieveiligheid.	**Ja**
Veilig personeel	**Ja**
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	**Ja**
Cryptografie	**Ja**
Fysieke beveiliging en beveiliging van de omgeving	**Ja**
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	**Ja**
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	**Ja**

***** EINDE VAN DIT DOCUMENT *****