Handreiking Autorisatie tot het Elektronisch Patiëntendossier

Amersfoort, GGZ Nederland, maart 2014
Versie 1.1.

Brancheorganisatie voor de geestelijke gezondheids- en verslavingszorg
Piet Mondriaanplein 25 • 3812 GZ Amersfoort • Postbus 830 • 3800 AV Amersfoort • T 033 460 89 00 • KVK 40483580
info@ggznederland.nl • www.ggznederland.nl • IBAN: NL56 INGB 0687 2118 08 BIC: INGBNL2A • IBAN: NL08 ABNA 0408 3901 07 BIC: ABNANL2A

Inhoudsopgave

Artikelen

Artikel 1

In deze handreiking wordt verstaan onder:
Elektronisch patiëntendossier: een elektronisch patiëntendossier (EPD) is een softwaretoepassing waarin diagnostische, medische en paramedische gegevens van één of meerdere personen worden opgeslagen, bewerkt en ingezien.[1]
Autorisatie: een softwaretoepassing in het EPD dat de machtiging voor toegang tot en het gebruik van het EPD regelt.[2]
Verantwoordelijke: de raad van bestuur van de zorginstelling die de middelen voor de verwerking van persoonsgegevens vaststelt.[3]
Logging: het vastleggen van wie wanneer het EPD heeft ingezien.[4]
Controle: het controleren van de loggegevens op onrechtmatige toegang.
Noodknop: mogelijkheid voor een gebruiker om in het EPD gegevens in te zien waarvoor hij niet geautoriseerd is.
Betrokkene: degene van wie persoonsgegevens in het EPD worden opgeslagen.
Zorgmedewerker: medewerker direct betrokken bij de zorgverlening aan[5] of behandeling van patiënten.

Artikel 2

1. De autorisatie tot het elektronisch patiëntendossier moet zodanig zijn vormgegeven dat alleen bevoegde medewerkers er toegang toe hebben en er bewerkingen in kunnen uitvoeren.

2. Bevoegde medewerkers zijn de zorgmedewerkers die rechtstreeks bij de behandeling van de betreffende patiënt betrokken zijn en degenen die optreden als intern vervanger van de zorgmedewerker.
Daarnaast zijn alle andere medewerkers bevoegd, wanneer het noodzakelijk is voor het beheer van de instelling of de beroepspraktijk[6].
3. De autorisatie beperkt zich tot hetgeen dat noodzakelijk is voor de door bevoegde medewerkers te verrichten werkzaamheden.
4. Er moet een autorisatiebeleid aanwezig zijn waarin de specifieke vormgeving van de autorisatie tot het EPD wordt beschreven en onderbouwd. Hiermee wordt beoogd de technische autorisaties te laten overeenstemmen met de vanuit de functie van de medewerker bezien noodzakelijke en daardoor rechtmatige toegang.

---

[1] Zie ook NEN 7510:2011, m.n. p. 11, §2.30
[2] Zie ook de ontwerpnorm NEN 7521:2014 voor aanwijzingen voor het inrichten en gebruik van een systeem van toegang tot patientgegevens.
[3] Zie ook College Bescherming Persoonsgegevens, Onderzoeksrapport '*Toegang tot digitale patiëntendossiers binnen zorginstellingen',* juni 2013, p. 6.
[4] Zie ook NEN 7513:2010, voor aanwijzingen voor het loggen en gebruik van de logging om te voldoen aan wettelijke verplichtingen en levert ontwikkelaars van informatiesystemen een aantal eisen waaraan hun systemen zullen moeten voldoen.
[5] Hiermee wordt, conform de definitie uit NEN 7510, bedoeld: het doen van onderzoek, het geven van raad en het uitvoeren van handelingen op het gebied van de gezondheidszorg.
[6] Met beroepspraktijk wordt hier een samenwerkingsverband bedoeld.

Artikel 3

1. Bij wijze van uitzondering kan op functie- of afdelingsniveau structureel worden afgeweken van het bepaalde in artikel 2 lid 1.

2. Van een uitzondering op functie- of afdelingsniveau kan sprake zijn bij een behandeling met een spoedeisend en/of complex karakter, waarvoor toegang tot de patiëntgegevens essentieel is voor het waarborgen van de kwaliteit en/of continuïteit van zorg.

3. Indien de actuele stand van de technische mogelijkheden niet zo ver strekt, of niet in redelijke verhouding staan tot de kosten- en arbeidsintensiteit dat uitbuiting van deze mogelijkheden vergt, dat geautoriseerd kan worden op behandelrelatie, kan ook structureel op functie- of afdelingsniveau worden afgeweken van het bepaalde in artikel 2 lid 1.

4. Alle afwijkingen op functie- of afdelingsniveau van het bepaalde in artikel 2 lid 1 in verband met de hierboven in lid 1 t/m 3 beschreven gronden zijn alleen toegestaan met inachtneming van de eisen van proportionaliteit en redelijkheid, en dienen te worden gemotiveerd. Daarnaast moet er altijd worden gestreefd naar autorisatie van een zo klein mogelijke schakel rondom de patiënt.

Artikel 4

Er moet structureel worden bijgehouden en geregistreerd in een logbestand wie wanneer het EPD heeft ingezien.

Artikel 5

1. De logbestanden moeten periodiek worden gecontroleerd op indicaties van onrechtmatige toegang tot de gegevens in het EPD.

2. Indien nodig moet de verantwoordelijke actie ondernemen om de onrechtmatige toegang terug te dringen, te stoppen of te voorkomen.

Artikel 6

1. Er moeten technische en organisatorische maatregelen worden genomen

a. om de autorisatie in het EPD te regelen volgens de in artikel 2 gegeven voorwaarden
b. om logbestanden te creëren zoals beschreven in artikel 4
c. om de logbestanden te controleren zoals beschreven in artikel 5.1.

2. De te nemen technische en organisatorische maatregelen worden opgesteld en geïmplementeerd met inachtneming van de stand van de techniek en de kosten van de tenuitvoerlegging.

Algemene Toelichting

Aanleiding voor deze handreiking

Zorginstellingen werken met elektronische patiëntendossiers (epd's). Dit kan de effectiviteit en efficiëntie van de hulpverlening ten goede komen, doordat bij juist gebruik de gegevens in het dossier makkelijker en sneller beschikbaar zijn, ook in geval van nood.
Het werken met digitale patiëntendossiers kent ook risico's. Deze risico's bevinden zich onder meer op het vlak van privacy: de elektronische toegang tot de dossiers verhoogt de kans dat de gegevens toegankelijk zijn voor onbevoegden.
Bevoegden zijn volgens de wet zorgmedewerkers die rechtstreeks bij de behandeling van de patiënt betrokken zijn en medewerkers voor wie het in verband met hun functie in het beheer van de instelling noodzakelijk is om toegang tot het dossier te hebben.
Het is de verantwoordelijkheid van het bestuur van een zorginstelling ervoor zorg te dragen dat de privacy van de patiënten is gewaarborgd en dat er zorgvuldig met de medische gegevens wordt omgegaan en alleen bevoegden toegang tot deze gegevens hebben. Het is belangrijk dat de patiënt hierop kan vertrouwen.
Helaas blijkt uit onderzoek van het College Bescherming Persoonsgegevens (CBP)[7] – die de zorgvuldige omgang met medische gegevens hoog op de toezichtagenda heeft staan – dat dit in de praktijk lang niet altijd het geval is. De manier waarop zorginstellingen de toegang van medewerkers tot digitale patiëntendossiers en de beveiliging van de gegevens hebben geregeld bleek naar het oordeel van het CBP niet te voldoen aan de eisen uit de Wet bescherming persoonsgegevens (Wbp).
Deze handreiking maakt duidelijk aan welke eisen de autorisatie tot het elektronisch patiëntendossier moet voldoen. Het is bedoeld als praktisch hulpmiddel waarmee GGZ Nederland haar leden wil ondersteunen. De handreiking gaat naast de geldende wetgeving ook uit van andere documenten (zie hiervoor de bronnenlijst in de bijlage) en is van toepassing op ggz instellingen die zijn aangesloten bij GGZ Nederland.

[7] CBP, Onderzoeksrapport '*Toegang tot digitale patiëntendossiers binnen zorginstellingen*', juni 2013.

Artikelsgewijze Toelichting

Artikel 1
Dit artikel bevat de definitie van de belangrijkste begrippen die in deze handreiking worden gehanteerd.

Artikel 2
Dit artikel gaat over de wijze van autoriseren.
De wet bepaalt dat alleen die zorgmedewerkers die rechtstreeks bij de behandeling van de patiënt betrokken zijn toegang tot het dossier mogen hebben. Daarnaast is toegang door overige medewerkers toegestaan wanneer dit noodzakelijk is voor het beheer van de instelling of de beroepspraktijk. Het begrip beheer moet beperkt worden uitgelegd en betreft ofwel verwerkingen ten behoeve van het waarborgen van de kwaliteit van zorg[8] ofwel verwerkingen die rechtstreeks verband houden met de financiële afhandeling van de medische behandeling. Voor alle andere activiteiten die in het kader van het beheer moeten worden uitgevoerd mag in principe slechts gebruik gemaakt worden van gegevens van niet geïdentificeerde of identificeerbare personen.[9] Er zijn echter werkzaamheden denkbaar die onmogelijk kunnen worden uitgevoerd zonder toegang tot geïdentificeerde of identificeerbare gegevens. Dit geldt bijvoorbeeld voor het op verzoek van de patiënt verwijderen van het dossier door applicatiebeheerders. Wanneer er in een dergelijk geval gebruik wordt gemaakt van gegevens uit het EPD, is het van belang dat de reden hiervoor wordt gemotiveerd. Hierbij moet ook moet ook de proportionaliteit in acht genomen worden: is er echt sprake van noodzakelijke toegang tot de gegevens? En zo ja, door bijvoorbeeld de gehele administratieve afdeling of slechts voor één bepaalde medewerker? Etc.

Er moeten procedures worden opgesteld waarin is vastgelegd wie onder welke omstandigheden toegang heeft tot welke gegevens. Instellingen kunnen dit op een eigen, onderbouwde wijze vormgeven, en kan bijvoorbeeld inhouden dat er profielen met bepaalde bevoegdheden worden opgesteld, die worden gekoppeld aan het personeelsnummer en de functie van een medewerker.
Ook moet er voorzien worden in technische maatregelen die voorkomen dat onbevoegden toegang tot de gegevens hebben en mogelijk maken dat de bevoegden dat wél hebben. Toegang mag pas worden verleend wanneer is vastgesteld dat er sprake is van rechtstreekse betrokkenheid bij de behandeling van de patiënt of als dit noodzakelijk is voor werkzaamheden in het kader van het beheer van de instelling of beroepspraktijk. Hiervoor is eerst nodig dat duidelijk is welke personen rechtstreeks bij de behandeling betrokken zijn. Volgens de Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst (KNMG) zijn dit medewerkers "die op grond van geldende wet- en regelgeving een medisch inhoudelijke rol vervullen bij de behandeling van de patiënt, zoals apothekersassistenten, doktersassistenten c.q. praktijkassistenten, laboranten en arts-assistenten"[10] of medewerkers "die als team, op gelijkgerichte wijze, betrokken zijn bij het doel waarvoor de gegevens

[8] Hieronder worden begrepen: verwerkingen noodzakelijk voor de uitvoering van de behandeling als zodanig, en verwerkingen noodzakelijk voor intercollegiale toetsing van wat in het vervolg beter kan.
[9] Sdu Commentaar, 'Wet bescherming persoonsgegevens', 2011, p. 83; Mvt op Wbp, p. 110.
[10] KNMG, Modelrichtlijn en Modelvoorlichtingsmateriaal Autorisatie voor Koplopers Elektronisch Medicatie Dossier, 2005, p. 10.

worden verstrekt.”.[11]
Deze definitie is – waarschijnlijk ingegeven door de beroepsgroep voor wie de richtlijnen van de KNMG zijn geschreven - duidelijk toegespitst op artsen en andere medewerkers met een medisch inhoudelijke rol. Natuurlijk kunnen ook individuele zorgmedewerkers zonder medisch inhoudelijke rol, zoals bijvoorbeeld de maatschappelijk werker rechtstreeks bij de behandeling betrokken zijn en dus toegang tot het dossier verleend krijgen.
Daarnaast moet duidelijk zijn voor welke gegevens toegang mag worden verleend. De rechtstreeks bij de behandeling betrokkenen hebben toegang tot alle gegevens die noodzakelijk zijn voor de door hen te verrichten werkzaamheden.
Voor degenen die uit noodzaak voor het beheer van de instelling of de beroepspraktijk toegang hebben tot het EPD, geldt ook dat zij slechts toegang hebben tot die gegevens waarvoor de noodzaak tot toegang bestaat.

Artikel 3
Dit artikel gaat over de mogelijkheid tot afwijken van het bepaalde in artikel 2 lid 1.
Uit sommige behandelingen met een spoedeisend en/of complex karakter kan een reëel gevaar voor de patiëntveiligheid of voor continuïteit van de zorg voortvloeien indien (een) bepaalde zorgmedewerker(s) geen toegang tot de medische gegevens zou(den) hebben.
In die gevallen kan het bij wijze van uitzondering noodzakelijk zijn om op functie- of afdelingsniveau van artikel 2 lid 1 af te wijken. Zo kan het bijvoorbeeld op een klinische afdeling, waar in een klein wisselend team 24/7 zorg geboden wordt noodzakelijk zijn om de gehele afdeling te autoriseren voor iedere patiënt op die afdeling, terwijl de autorisatie zo is vormgegeven dat alleen direct bij de behandeling betrokken medewerkers toegang tot het EPD hebben.
Daarnaast moet bij de autorisatie rekening worden gehouden met wat technisch en organisatorisch mogelijk is binnen de betreffende ggz instelling en of het uitbuiten van de mogelijkheden in redelijke verhouding staat met de kosten- en arbeidsintensiteit dat dit vergt.
Met als uiteindelijke doel de autorisatie van slechts diegenen die rechtstreeks bij de behandeling van de patiënt betrokken zijn en van degenen voor wie toegang tot het EPD gezien hun werkzaamheden noodzakelijk is voor het beheer van de instelling of beroepspraktijk, moet er naar gestreefd worden een zo klein mogelijke schakel rondom de patiënt de autoriseren, dit kan bijvoorbeeld de afdeling waarop de patiënt wordt behandeld of begeleid zijn. Indien dit technisch en organisatorisch het hoogst haalbare is, zal dit in afwijking van het bepaalde van artikel 2 lid 1 het uitgangspunt moeten zijn voor de vormgeving van de autorisaties.

Voor iedere afwijking van het bepaalde in artikel 2 – individueel of op afdelingsniveau – geldt dat proportioneel en redelijk moet worden gehandeld, en dat deze gemotiveerd moet worden.
NB: Er kunnen zich ook situaties voordoen waarbij een zorgmedewerker zonder autorisatie direct bij de behandeling betrokken raakt en vanuit die positie informatie uit het EPD nodig heeft. Als het gaat om een acute situatie zal er geen tijd zijn om voor deze medewerker een autorisatie in te stellen in het EPD. Om voor deze medewerker toch tijdelijke toegang tot het EPD mogelijk te maken, kan een zogenaamde ‘noodknop’ in het EPD worden ingebouwd. Een zorgmedewerker die zich ondanks ontbrekende of ontoereikende autorisatie toegang tot het dossier wil verschaffen, kan hier dan gebruik van maken. Om misbruik van deze mogelijkheid tegen te gaan, kan er bijvoorbeeld gebruik gemaakt worden van een drop-down

[11] KNMG, Richtlijn inzake het Omgaan met Medische Gegevens, 2010, p. 21.

venster met mogelijke verantwoordingen voor het gebruik van de noodknop, waarvan de medewerker er één moet kiezen.

Artikel 4

In dit artikel wordt bepaald dat de verantwoordelijke structureel moet bijhouden wie wanneer een dossier raadpleegt.

Logging moet het mogelijk maken om eventuele onbevoegd verkregen toegang te achterhalen en aan de hand hiervan maatregelen te nemen.
De logbestanden moeten daarom inzage geven in wie toegang tot het dossier op hoofdniveau en tot de afzonderlijke mappen daarbinnen heeft gehad.
Het is niet noodzakelijk om ook de inhoud van die bewerkingen bij te houden en te registeren.

Artikel 5

In dit artikel wordt bepaald dat de logbestanden periodiek moeten worden gecontroleerd op indicaties van onrechtmatige toegang tot het EPD en dat waar nodig actie moet worden ondernomen.
Periodiek moet worden gecontroleerd of de autorisaties juist zijn verstrekt. Dit kan door bijvoorbeeld steekproefsgewijs te controleren of de technische autorisatie van medewerkers wel overeen komt met wat bezien vanuit hun functie noodzakelijk en daarom rechtmatig is. Daarnaast dienen er – bijvoorbeeld naar aanleiding van een klacht van een patiënt - reactieve controles plaats te vinden.
Ook het gebruik van de noodknopprocedure moet periodiek worden gecontroleerd. Het is hierbij praktisch gezien ondoenlijk om na te gaan of iedere opgegeven verantwoording voor het gebruik van de noodknop daadwerkelijk aan de orde was, dit kan dan ook achterwege gelaten worden.
Wel moet worden gecontroleerd op afwijkend gebruik van de noodknop. Wat geldt als afwijkend gebruik hangt af van verschillende omstandigheden. Bepalend is onder andere hoe een instelling de autorisatie heeft geregeld en hoe de functies en behandelteams zijn samengesteld. Zo zal het gebruik van de noodknop bij een instelling die haar FACT-teams bij wijze van uitzondering[12] op teamniveau heeft geautoriseerd nogal afwijken van het gebruik bij een instelling die dat niet heeft gedaan.

De controle op de logging vindt bij voorkeur plaats door een andere medewerker dat degene(n) die de logbestanden genereert.

Artikel 6

Dit artikel benadrukt nogmaals dat bij het opstellen van technische en organisatorische maatregelen om de autorisatie, het loggen en de controle vorm te geven, rekening moet worden gehouden met de stand van de techniek en de kosten voor de tenuitvoerlegging van de betreffende maatregelen.

[12] Vanwege het complexe karakter van de door FACT-teams geboden zorg, kan het noodzakelijk zijn voor de borging van de kwaliteit en continuïteit van zorg om het gehele team structureel volledige toegang tot het dossier de door hen te behandelen patiënt(en) te verschaffen.

De technische en organisatorische maatregelen dienen cumulatief te worden getroffen, het is dus niet óf/óf.
Bij het treffen van de benodigde maatregelen moeten de technische inspanning en de kosten in redelijke verhouding tot het doel staan. Het is dan ook niet verplicht het allerzwaarst mogelijke beveiligingsniveau te hanteren: waar het om gaat is dat er sprake moet zijn van een adequate beveiliging.[13]

Binnen de ggz worden door instellingen maatregelen geïmplementeerd die voortvloeien uit bijvoorbeeld de regels omtrent het beroepsgeheim en cao-bepalingen. Ook de HKZ-normen en NEN-normen maken veelal deel uit van het beleid.
Naast deze waarborgen voor de bescherming van de persoonsgegevens van de betrokkenen dient ook een specifiek autorisatiebeleid met daarin een omschrijving van technische en organisatorische maatregelen ter bescherming van de gegevens in het EPD aanwezig te zijn en gehanteerd te worden. Bij het opstellen van dit beleid kan deze handreiking als uitgangspunt genomen worden.

[13] Zie ook Sdu Commentaar, 'Wet bescherming persoonsgegevens', 2011, p. 66.

Bijlage I: Geldende wetgeving

Hieronder volgen een aantal artikelen welke bij het schrijven van de onderhavige handreiking als basis hebben gediend.

Artikel 7:457 Burgerlijk Wetboek (BW)
1. Onverminderd artikel 448, derde lid, tweede volzin, draagt de hulpverlener zorg dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking kan geschieden zonder inachtneming van de beperkingen, bedoeld in de voorgaande volzinnen, indien het bij of krachtens de wet bepaalde daartoe verplicht.
2. Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden.
3. Daaronder zijn evenmin begrepen degenen wier toestemming ter zake van de uitvoering van de behandelingsovereenkomst op grond van de artikelen 450 en 465 is vereist. Indien de hulpverlener door inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege.

Artikel 7:458 BW
1. In afwijking van het bepaalde in artikel 457 lid 1 kunnen zonder toestemming van de patiënt ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid aan een ander desgevraagd inlichtingen over de patiënt of inzage in de bescheiden, bedoeld in artikel 454, worden verstrekt indien:
a. het vragen van toestemming in redelijkheid niet mogelijk is en met betrekking tot de uitvoering van het onderzoek is voorzien in zodanige waarborgen, dat de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad, of
b. het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener zorg heeft gedragen dat de gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.
2. Verstrekking overeenkomstig lid 1 is slechts mogelijk indien:
a. het onderzoek een algemeen belang dient,
b. het onderzoek niet zonder de desbetreffende gegevens kan worden uitgevoerd, en
c. voor zover de betrokken patiënt tegen een verstrekking niet uitdrukkelijk bezwaar heeft gemaakt.
3. Bij een verstrekking overeenkomstig lid 1 wordt daarvan aantekening gehouden in het dossier.
Artikel 13 Wet bescherming persoonsgegevens (Wbp)
De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De

maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 16 Wbp
De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Artikel 21 Wbp
1. Het verbod om persoonsgegevens betreffende iemands gezondheid te verwerken als bedoeld in artikel 16, is niet van toepassing indien de verwerking geschiedt door:
a. hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is;
b. verzekeraars als bedoeld in artikel 1:1 van de Wet op het financieel toezicht en financiële dienstverleners die bemiddelen in verzekeringen als bedoeld in artikel 1:1 van die wet, voorzover dat noodzakelijk is voor:
1°. de beoordeling van het door de verzekeraar te verzekeren risico en de betrokkene geen bezwaar heeft gemaakt; of
2°. de uitvoering van de overeenkomst van verzekering;
c. scholen voor zover dat met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is;
d. een reclasseringsinstelling, een bijzondere reclasseringsambtenaar, de raad voor de kinderbescherming of de stichting, bedoeld in artikel 1, onder f, van de Wet op de jeugdzorg en de rechtspersoon, bedoeld in artikel 254, tweede lid, of artikel 302, tweede lid, van Boek 1 van het Burgerlijk Wetboek, voor zover dat noodzakelijk is voor de uitvoering van de hun wettelijk opgedragen taken;
e. Onze Minister voor zover dat in verband met de tenuitvoerlegging van vrijheidsstraffen of vrijheidsbenemende maatregelen noodzakelijk is of
f. bestuursorganen, pensioenfondsen, werkgevers of instellingen die te hunnen behoeve werkzaam zijn voor zover dat noodzakelijk is voor:
1°. een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene of
2°. de reïntegratie of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.
2. In de gevallen als bedoeld in het eerste lid worden de gegevens alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht. Indien de verantwoordelijke gegevens persoonlijk verwerkt en op hem niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht rust, is hij verplicht tot geheimhouding van de gegevens, behoudens voor zover de wet hem tot mededeling verplicht of uit zijn taak de noodzaak voortvloeit dat de gegevens worden meegedeeld aan anderen die krachtens het eerste lid bevoegd zijn tot verwerking daarvan.
3. Het verbod om andere persoonsgegevens als bedoeld in artikel 16 te verwerken, is niet

van toepassing voor zover dit noodzakelijk is in aanvulling op de verwerking van persoonsgegevens betreffende iemands gezondheid als bedoeld in het eerste lid, onder a, met het oog op een goede behandeling of verzorging van de betrokkene.
4. Persoonsgegevens betreffende erfelijke eigenschappen mogen slechts worden verwerkt voor zover deze verwerking plaatsvindt met betrekking tot de betrokkene bij wie de betreffende gegevens zijn verkregen, tenzij:
a. een zwaarwegend geneeskundig belang prevaleert of
b. de verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek of statistiek.
In het geval als bedoeld onder b, is artikel 23, eerste lid, onder a, en tweede lid, van overeenkomstige toepassing.
5. Bij algemene maatregel van bestuur kunnen omtrent de toepassing van het eerste lid, onder b en f, nadere regels worden gesteld.

Bijlage II: Bronnen

CBP 2013
CBP, Onderzoeksrapport 'Toegang tot digitale patiëntendossiers binnen zorginstellingen', 2013.
KNMG 2005
KNMG, Modelrichtlijn en Modelvoorlichtingsmateriaal Autorisatie voor Koplopers Elektronisch Medicatie Dossier, 2005.

KNMG 2010
KNMG, Richtlijn inzake het Omgaan met Medische Gegevens, 2010.
NEN 2010
NEN 7513:2010, Medische informatica - Logging - Vastleggen van acties op elektronische patiëntdossiers, 2010.
NEN 2011
NEN 7510:2011, Medische informatica - Informatiebeveiliging in de zorg, 2011.

NEN 2014
Ontwerpnorm NEN 7521:2014, Medische informatica - Toegang tot patiëntgegevens - Grondslagen voor uitwisseling, 2014.
Sdu Commentaar 2011
Sdu Commentaar, Wet bescherming persoonsgegevens, 2011.