Titel	**Gedragscode: informatieveiligheid (NEN 7.1.3 / 8.1 / 8.1.3) 0**
Locatie	**Purmerend én Hoorn**

Toepassingsgebied

Alle locaties van het Dijklander Ziekenhuis

Doel

Instructies geven en bewustwording vergroten, over informatieveiligheid en de wijze waarop gebruik moet worden gemaakt van informatiesystemen, inclusief e-mail, internet en telefonie in het Dijklander Ziekenhuis en sancties bij overtredingen

Doelgroep

Iedereen die werkzaam is in het Dijklander Ziekenhuis (zowel dienstverband, vrijgevestigd, gedetacheerd, uitzendkracht ZZP'er etc.)

Ziekenhuisbreed geldend

Ziekenhuisbreed geldend

Toelichting/ definities

Informatiebeveiliging van patiëntengegevens vormt een integraal onderdeel van het Dijklander Ziekenhuis, het legt een basis voor goede zorg voor patiënten.
De procedure garandeert adequate informatiebeveiliging van patiëntgegevens en de privacy van de patiënt.
Door bewustzijn en risicobeleving op dit gebied te creëren bij medewerkers zal de vertrouwelijkheid van onder andere patiëntgegevens beter gewaarborgd worden. Het tot een minimum beperken van risico's; zoals het onbevoegd veranderen van informatie in patiëntendossiers.
Bij het opstellen van deze gedragscode is voorop gesteld dat de regels werkbaar moeten zijn en niet bedoeld zijn om de medewerker in zijn dagelijkse werkzaamheden te beperken.
Het creëert een evenwicht tussen het praktisch beschikken over vertrouwelijke gegevens en beschermen van vertrouwelijke gegevens.

Werkwijze

Doelgroep/werkingssfeer/reikwijdte

Deze gedragscode is van toepassing op alle medewerkers (ook inhuur, PNIL) van het Dijklander Ziekenhuis.

Onder 'medewerker' wordt verstaan: iedereen die werkzaamheden voor het Dijklander Ziekenhuis verricht en daarbij kan beschikken over internet-, e-mailfaciliteiten en/of telefoniesystemen en -voorzieningen. Deze gedragscode maakt onderdeel uit van het informatiebeveiligingsbeleid (Informatiebeveiligingsbeleid 2019 - 2024 en is van toepassing op iedereen die gebruik maakt van informatievoorzieningen aangeboden door (een onderdeel van) het Dijklander Ziekenhuis onder wie personeelsleden, in het ziekenhuis werkzame vrijgevestigde medisch specialisten, medewerkers die werkzaam zijn voor vrijgevestigde medisch specialisten of een medisch specialistisch bedrijf (MSB) dat met het Dijklander Ziekenhuis samenwerkt, gedetacheerden, uitzendkrachten, studenten, stagiaires, oproepkrachten, vrijwilligers en medewerkers van externe partijen.

Deze gedragscode beschrijft de gedragsregels voor individuele gebruikers van informatievoorzieningen en -systemen met betrekking tot patiëntengegevens en bedrijfsinformatie van het Dijklander Ziekenhuis.

Onder 'informatiebeveiliging' wordt verstaan: het stelsel van maatregelen voor het behoud van vertrouwelijkheid, integriteit en beschikbaarheid van gegevens, processen en informatiesystemen.

Onder 'informatiesysteem' wordt verstaan: het geheel van mensen, middelen, procedures en regels dat de informatievoorziening verzorgt. Deze set van componenten heeft als doel informatie te verzamelen, verwerken, opslaan en verspreiden ter ondersteuning van de zorg, besluitvorming, coördinatie en controle binnen de organisatie.

Algemeen

De medewerker dient zich te houden aan de wet- en regelgeving met betrekking tot informatiebeveiliging, zoals (niet-limitatief) de regels die zijn vastgelegd in bijvoorbeeld de Algemene verordening gegevensbescherming (AVG), Wet meldplicht datalekken, de Wet geneeskundige behandelingsovereenkomst (WGBO) en de NEN 7510 .

Het Dijklander Ziekenhuis beoogt met deze gedragscode:

- Instructies te geven over wijze waarop gebruik moet worden gemaakt van informatiesystemen zoals de applicaties waarin patiëntengegevens en bedrijfsinformatie worden verwerkt alsmede de internet-, e-mail- en telefoniefaciliteiten;
- De bewustwording te vergroten van de risico's verbonden aan het gebruik van informatiesystemen zoals applicaties waarin patiëntengegevens en bedrijfsinformatie worden verwerkt alsmede internet, e-mail en (mobiele) telefonie;
- De bewustwording te vergroten ten aanzien van het zorgvuldig omgaan met vertrouwelijke gegevens/persoonsgegevens en de daaraan verbonden risico's met name voor de privacy van de patiënt, het foutloze verloop van het zorgproces en de betrouwbaarheid van de patiëntengegevens;
- De bewustwording te vergroten hoe zorgvuldig om te gaan met bedrijfsgevoelige informatie;
- Eventuele negatieve gevolgen van het gebruik van informatie en informatiesystemen zoals het risico op computervirussen of het schenden van de privacy van de patiënt voor het Dijklander Ziekenhuis te voorkomen en/of te beperken.
- Imagoschade voorkomen en sancties opleggen bij overtredingen.

Uitgangspunt blijft een werkbare situatie voor medewerkers waarbij er op een veilige wijze met informatie wordt omgegaan.

Regels voor het gebruik van informatiesystemen

Internet

De informatiesystemen, e-mailfacilteiten en de internettoegang worden aan de medewerker voor zakelijk gebruik beschikbaar gesteld. Gebruik is dus onlosmakelijk verbonden met de taken die voortvloeien uit de functie.

Hoewel de toegang tot het internet bestemd is voor zakelijk gebruik is een kortstondig persoonlijk gebruik van het internet tijdens een pauze toegestaan mits dit niet storend is voor de dagelijkse werkzaamheden en het geen verboden gebruik oplevert. Bij twijfel wordt de medewerker geacht overleg te plegen met de leidinggevende over het privé gebruik.

Het is niet toegestaan om via de internetfaciliteiten van het Dijklander Ziekenhuis:

- sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten. Hieronder vallen ook erotisch getinte sites en datingsites. Ook het bezoeken van sites die bestemd zijn om te gokken en/of geld te verwerven dan wel het bezoeken van chat - en babbelboxen is niet toegestaan;
- materiaal te downloaden waarvan de gebruiker redelijkerwijs kan begrijpen dat het ziekenhuis zich daar niet mee kan verenigen of de goede naam van de zorginstelling schaadt;
- sites te bezoeken die met name bedoeld zijn voor ontspanning en vermaak met spelletjes, puzzels, muziek etc.;
- zich ongeoorloofd toegang te verschaffen tot niet-openbare bronnen op internet;
- zich onbevoegd toegang te verschaffen tot systemen van andere organisaties;
- het e-mailadres en de naam van het ziekenhuis achter te laten op websites, tenzij hiertoe toestemming is verkregen van de leidinggevende;
- materiaal te downloaden en/of te installeren op de computer. Deze mogelijkheid is centraal zoveel mogelijk geblokkeerd. Indien het downloaden en/of installeren van materiaal voor de functie noodzakelijk is, dan is het verplicht dit te melden bij de supportdesk ICT en ten aanzien van de betrokken applicatie een risicoanalyse uit te voeren.
- software, gegevens of artikelen te downloaden of te kopiëren waarvoor licenties of auteursrechten gelden;
- bestanden vanuit het Dijklander Ziekenhuis te uploaden naar of beschikbaar te stellen aan derden buiten het netwerk van het ziekenhuis behalve in de situaties waarin daartoe een wettelijke verplichting bestaat.

E-mail

Het volledig veilig verzenden van e-mail berichten is gegarandeerd binnen het netwerk van het Dijklander Ziekenhuis en naar de veilige adressen via (http://www.zorgring.nl/diensten/veilig-mailen/) de Stichting Zorgring NHN. Buiten het netwerk van het Dijklander Ziekenhuis - dit geldt ook voor de webmail - kan het veilig verzenden van e-mail berichten niet worden gegarandeerd en in beginsel niet toegestaan.

Het e-mailadres is bedoeld voor zakelijk gebruik.
Medewerkers worden geacht hier met alle mogelijke voorzichtigheid mee om te gaan en in ieder geval de volgende zaken in acht te nemen:

- De medewerker is persoonlijk verantwoordelijk voor het gebruik van de aan hem of haar toegekende rechten voor systemen en middelen;
- Patiënt gerelateerde en/of bedrijfsgevoelige informatie mag niet per e-mail vanuit het Dijklander Ziekenhuis naar buiten worden verstuurd, tenzij het bericht op zodanige wijze is versleuteld dat de gegevens niet herleidbaar zijn;
- Bij patiënt gerelateerde informatie die direct tot de persoon herleidbaar is, dient de verzender zich ervan vergewist te hebben dat de ontvanger de privacy van de patiënt zal waarborgen;
- Patiëntengegevens mogen niet via een andere mailserver (zoals hotmail, Gmail e.d.) dan die van het ziekenhuis verstuurd worden;
- Het is de medewerker niet toegestaan om aan derden (gedeelten van) het interne Dijklander Ziekenhuis adresboek met e-mailadressen beschikbaar te stellen.

Het is niet toegestaan om via de e-mailfaciliteiten van het Dijklander Ziekenhuis:

- Berichten anoniem of onder een fictieve naam te versturen.
- Ketting e-mailberichten te verzenden of door te sturen.
- Ten behoeve van privé-gebruik abonnementen te nemen op nieuwsbrieven c.q. deel te nemen aan nieuwsgroepen.

- Iemand lastig te vallen door middel van onnodige en/of ongewenste berichten.

Pushmail

Pushmail is de voorziening waarbij e-mail direct wordt gesynchroniseerd tussen de mail omgeving (exchange) en een mobiel device (smartphone/tablet), waardoor je overal en continu de beschikking hebt over de laatste informatie. Bij het synchroniseren met het netwerk van het Dijklander Ziekenhuis gaat de medewerker akkoord met de onderstaande uitgangspunten van het Dijklander Ziekenhuis:

- Het ziekenhuis mag en kan de synchronisatie met een privé apparaat (smartphone/Pad) direct stopzetten.
- Het ziekenhuis mag en kan het privé apparaat volledig wissen, inclusief privé data
- Het ziekenhuis mag en kan de gegevens inzien van het privé apparaat (smartphone/Pad) indien dit nodig is tijdens een onderzoek naar mogelijk misbruik.

Randvoorwaarden voor beschikbaarstelling:

- Pushmail wordt niet verplicht gesteld aan medewerkers en geschiedt op basis van vrijwilligheid. De leidinggevende is verantwoordelijk voor het aanvragen van de pushmail faciliteit bij ICT;
- Alleen medewerkers in vaste dienst komen in aanmerking voor het gebruik van pushmail. Uitzondering hierop zijn functionarissen die bepaalde sleutelposities bekleden (o.a. artsen, management/staf, hoofden) of bij functies waarbij 24/7 bereikbaarheid wordt verwacht. Zij kunnen ook bij een tijdelijk contract gebruik maken van deze service.
- Door het Dijklander Ziekenhuis, afdeling ICT, wordt bepaald voor welke devices pushmail ter beschikking wordt gesteld.

Randvoorwaarden en verantwoordelijkheden voor gebruikers:

- Medewerkers gaan zorgvuldig om met (vertrouwelijke) informatie. Pushmail is uitsluitend bedoeld voor zakelijk gebruik
- De beveiliging van pushmail mag niet worden uitgeschakeld of gewijzigd.
- Er dient een inlogcode/wachtwoord te zijn ingesteld op de mobiele device ter voorkoming van ongeautoriseerde toegang.
- Medewerkers dienen na het uitbrengen van (beveiligings)updates van de fabrikant deze zo spoedig mogelijk op het device te installeren.
- Ongewenst gebruik van informatie en communicatiemiddelen moet worden voorkomen. Het is niet toegestaan om e-mails te lezen en verwerken via een openbaar wifi netwerk, waarvan men niet weet wie de beheerder is en hoe het netwerk beveiligd is. De medewerker dient de device niet automatisch met openbare netwerken te laten verbinden. Wifi functionaliteit dient dan te worden uitgeschakeld om gebruik te maken van het mobiele netwerk van de eigen provider (4G/5G).
- Medewerkers zijn attent op de beveiliging en veiligheid. Zij zijn gehouden aan het geldende beleid om incidenten en kwetsbaarheden met betrekking tot beveiliging en gebruik van informatie en communicatiemiddelen onmiddellijk te melden bij zijn/haar leidinggevende en een incidentmelding informatiebeveiliging aan te maken via IProva.
- Verlies en/of diefstal van een device waar pushmail op aanwezig is dient direct bij de supportdesk van de afdeling ICT gemeld te worden.

Randvoorwaarden en verantwoordelijkheden ziekenhuis:

- Bij melding van verlies/diefstal van het device zal een medewerker van afdeling ICT de pushmail faciliteit zo snel als mogelijk blokkeren. Technisch is het mogelijk om op afstand te kunnen ingrijpen op het device (z.g. remote wipe, waarmee je toegang tot de mail kunt wissen)
- Bij uitdiensttreding wordt de pushmail faciliteit na ontvangst van een uit dienst melding gedeactiveerd. Het afdelingshoofd is verantwoordelijk voor het doorgeven van de uitdiensttreding.

Gebruikersnaam / wachtwoorden

De gebruiker heeft toegang tot de ICT-voorzieningen door middel van een gebruikersnaam en wachtwoord. De gebruikersnaam en het wachtwoord zijn strikt persoonlijk en dienen uitsluitend gebruikt te worden door de betreffende medewerker om toegang te krijgen tot de systemen.

Het persoonlijke wachtwoord dat toegang geeft tot de ICT-voorzieningen kan bestaan uit een combinatie van numerieke en alfanumerieke tekens die toegang geven tot het netwerk en moet voldoen aan de wachtwoord policy van het Dijklander Ziekenhuis.
Voor de verschillende applicaties kunnen, door de applicatiebeheerders, aparte wachtwoorden uitgegeven worden volgens de daartoe opgestelde procedures en eisen.
Het wachtwoord dient regelmatig te worden gewijzigd. Het moment van wijziging wordt getoond bij het inloggen.

Het is niet toegestaan om gebruikersnamen en wachtwoorden van systemen van het Dijklander Ziekenhuis:

- Aan derden beschikbaar te stellen (met derden worden tevens andere medewerkers van het Dijklander Ziekenhuis bedoeld).
- Op een voor anderen of openbaar toegankelijke plek of anderszins onzorgvuldig te bewaren.
- Van andere medewerkers op enigerlei wijze en in enigerlei vorm te bemachtigen en/of te gebruiken.

De medewerker is gehouden de combinatie gebruikersnaam en wachtwoord(en) zorgvuldig te beheren. De medewerker blijft verantwoordelijk voor zijn/haar eigen wachtwoordgebruik.

Social media, blogs, wiki's, fora en andere media

Medewerkers moeten alle informatie vanuit het Dijklander Ziekenhuis beschouwen als vertrouwelijk tenzij uitdrukkelijk anders is bepaald.

Medewerkers zijn persoonlijk verantwoordelijk voor de inhoud die ze - voor zover dat niet tot hun functie behoort - publiceren op social media, blogs, wiki's, fora (zoals Facebook, LinkedIn, Snapchat, Twitter en Instagram) en andere media die gebaseerd zijn op user-generated content (= door gebruiker gemaakte inhoud)

Medewerkers zijn zich ervan bewust dat wat zij (privé) publiceren voor langere tijd openbaar zal worden, hetgeen mogelijk gevolgen kan hebben voor hun werksituatie. Medewerkers worden geacht hier met alle mogelijke voorzichtigheid mee om te gaan en in ieder geval de volgende zaken in acht te nemen:

- Over privacygevoelige en/of bedrijfsgevoelige informatie, waaronder patiëntengegevens, financiële gegevens en bijvoorbeeld incidenten en calamiteiten, wordt niet gepubliceerd.
- Medewerkers van het Dijklander Ziekenhuis respecteren degene tot wie zij zich richten binnen en buiten de werksituatie. Etnische laster, persoonlijke beledigingen en obsceniteit zijn niet geoorloofd. De privacy van anderen wordt gerespecteerd en de reputatie van het ziekenhuis wordt niet geschaad.
- Medewerkers die publiceren op een website anders dan die van het Dijklander Ziekenhuis over een onderwerp dat wel te maken kan hebben met het Dijklander Ziekenhuis, maken kenbaar dat zij op persoonlijke titel publiceren.
- Blogs en sociale netwerken die worden gehost door het Dijklander Ziekenhuis moeten worden gebruikt op een manier die waarde toevoegt aan de bedrijfsdoelstellingen en het imago van het Dijklander Ziekenhuis.
- Het maken van een selfie is toegestaan, mits dit de werkzaamheden niet hindert, niemand in beeld brengt die dat niet wenst en de privacy van anderen danwel de reputatie van het ziekenhuis niet schaadt.

Telefonie

Medewerkers mogen incidenteel en kortstondig de telefoon voorzieningen van het Dijklander Ziekenhuis gebruiken voor het voeren van privégesprekken, mits dit geen storende onderbreking vormt van de werkzaamheden en mits hierbij voldaan wordt aan de verdere richtlijnen van deze gedragscode.

Het is medewerkers in ieder geval verboden telefoons van het Dijklander Ziekenhuis te gebruiken om:

- servicenummers te bellen die beginnen met 0906 en 0909 anders dan voor doeleinden die voortvloeien uit de functie;
- internationale nummers te bellen voor privé-doeleinden;
- uitgaande telefoongesprekken te voeren die inhoudelijk strijdig zijn met wet- en regelgeving en de goede naam van het Dijklander Ziekenhuis op het spel zetten.

Medewerkers dienen zich ervan bewust te zijn dat een mobiele telefoon veel informatie kan bevatten waardoor de privacy van medewerkers en de patiënt in het geding kunnen komen. Medewerkers worden geacht hier met alle mogelijke voorzichtigheid mee om te gaan en in ieder geval de volgende zaken in acht te nemen:

- Het toestel zodanig bij zich dragen dat diefstal of verlies wordt voorkomen.
- In beginsel is het niet toegestaan om vertrouwelijke (persoons)gegevens en/of bedrijfsgevoelige informatie (zoals e-mail) op de telefoon op te slaan en wanneer dit wel voor het uitoefenen van de functie noodzakelijk is dienen de gegevens zodanig te worden versleuteld dat de privacy blijft gewaarborgd. Dit geldt tevens voor foto-, video- en geluidsopnames.
- Indien de mobiele telefoon vertrouwelijke gegevens/persoonsgegevens en/of bedrijfsgevoelige informatie bevat dient het bij vermissing of diefstal direct als veiligheidsincident gemeld te worden via IProva.

Mobiele gegevensdragers

Dossiers, papieren, DVD's, USB-memorysticks, laptops, notebooks, tablets en overige informatiedragers die vertrouwelijke (persoons)gegevens en/of bedrijfsgevoelige informatie bevatten, dienen met de grootst mogelijke zorgvuldigheid te worden bewaard. Het is in ieder geval niet toegestaan om opgeslagen bestanden op mobiele gegevensdragers die privacygevoelige informatie bevatten onbeheerd achter te laten, of niet goed genoeg te beschermen tegen verlies of diefstal.

Indien de mobiele gegevensdrager vertrouwelijke gegevens/ persoonsgegevens en/of bedrijfsgevoelige informatie bevat, dient dit bij vermissing of diefstal direct als veiligheidsincident gemeld te worden via IProva.

Hulpmiddelen voor toegang tot locaties

Medewerkers gebruiken de hulpmiddelen voor toegang tot locaties, apparatuur en ruimten van het Dijklander Ziekenhuis (zoals sleutels en pasjes) uitsluitend voor het doel waarvoor deze ter beschikking zijn gesteld. Medewerkers worden geacht hier met alle mogelijke voorzichtigheid mee om te gaan en in ieder geval de volgende zaken in acht te nemen:

- De medewerker probeert niet om onbevoegd toegang te krijgen tot locaties van het Dijklander Ziekenhuis.
- Voor de medewerker bestemde toegangsmiddelen zijn uitsluitend bedoeld voor persoonlijk gebruik en mogen niet beschikbaar worden gesteld aan collega's of andere derden, tenzij daarover andere schriftelijke afspraken zijn gemaakt met de leidinggevende en/of het Facilitair Servicepunt.

- Bij vermissing, ontvreemding, misbruik of ander onrechtmatig gebruik van personeelspas, sleutels, tags, toegangscodes, apparatuur of software stelt de medewerker de leidinggevende en het Facilitair Servicepunt onmiddellijk op de hoogte.

Privacy

Medewerkers dienen alle mogelijke middelen aan te wenden om de privacy van patiënten en van andere medewerkers te waarborgen. Aan derden worden geen gegevens over patiënten verstrekt tenzij dit noodzakelijk is voor de behandeling of aan de door patiënt aangewezen contactpersoon. In dat laatste geval is uitdrukkelijke toestemming nodig van betrokken patiënt.

Over medewerkers worden geen gegevens verstrekt aan derden of andere medewerkers. Vragen over medewerkers worden doorverwezen naar de HRM-afdeling.

Medewerkers dienen zich ervan bewust te zijn dat de nodige zorgvuldigheid dient te worden betracht bij het omgaan met vertrouwelijke gegevens/persoonsgegevens. Zij dienen in ieder geval de volgende zaken in acht te nemen:

- De werkplek dient op zodanige manier te zijn ingericht dat onbevoegden zich niet in afwezigheid van de medewerker toegang tot vertrouwelijke gegevens/persoonsgegevens kunnen verschaffen. Bij het verlaten van de werkplek dient de computer te worden geblokkeerd.
- Vertrouwelijke gegevens/persoonsgegevens worden niet onbeheerd achtergelaten op de balie, het bureau, de werkplek of in een niet-afsluitbare kast.
- In het Dijklander Ziekenhuis geldt het ‘clean-desk clear-screen’-beleid. Dit houdt in dat de medewerker zich ervan vergewist dat er geen vertrouwelijke gegevens/persoonsgegevens onbeheerd achtergelaten worden op de werkplek en het werkstation voorzien is van een werkende schermbeveiliging.

Alle vertrouwelijke gegevens/persoonsgegevens die worden opgeslagen, moeten zodanig worden beveiligd, dat verlies of onrechtmatig gebruik van de gegevens wordt voorkomen.

- Hiertoe is degene die de gegevens opslaat verplicht de noodzakelijke technische en organisatorische maatregelen te treffen. Dit geldt ook voor elektronisch opgeslagen vertrouwelijke gegevens/persoonsgegevens.
- Bij online uitwisseling van gegevens dient de medewerker maatregelen te treffen die de privacy van de patiënt waarborgen tijdens het transport van de gegevens en bij de andere partij. Hierbij dienen gegevens minimaal versleuteld verstuurd te worden.

Om de privacy van de patiënten van het Dijklander Ziekenhuis te kunnen waarborgen, is het niet toegestaan om foto-, film- of geluidsopnamen te maken in het Dijklander Ziekenhuis en op het terrein van het Dijklander Ziekenhuis zonder uitdrukkelijke toestemming van de daartoe bevoegde personen in het Dijklander Ziekenhuis alsmede de betreffende patiënt(en). Onder opname wordt verstaan alle vormen van geluid- en/of beeldregistratie.

Het is medewerkers niet toegestaan de door het Dijklander Ziekenhuis ter beschikking gestelde programmatuur, databestanden en documentatie te kopiëren of ter beschikking te stellen aan derden, behoudens i.g.v. daartoe verleende (schriftelijke) toestemming.

Melden van incidenten (inclusief datalekken) en zwakke plekken in informatiesystemen

Medewerkers moeten incidenten m.b.t. Informatiebeveiliging (inclusief datalekken) en zwakke plekken in ICT-voorzieningen of informatiesystemen, die (potentieel) een inbreuk vormen op de gestelde beveiligingsnormen zo snel mogelijk melden via een datalekmelding in Iprova.

Zwakke plekken in (informatie)systemen mogen door medewerkers niet worden gedemonstreerd behalve aan de medewerkers van de ICT afdeling of de CISO van het Dijklander Ziekenhuis.
De registratie van de melding gebeurt primair om de kwaliteit van de zorg te verbeteren en om het beheer, de continuïteit, de veiligheid, de integriteit en de beschikbaarheid van de infrastructuur en de diensten te waarborgen, alsmede om verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan.

Controle

Van alle medewerkers wordt verwacht dat zij zich actief inspannen om informatie(systemen) te beveiligen in het eigen belang en in het belang van het ziekenhuis.

Informatiebeveiliging is een integraal onderdeel van de normale werkzaamheden en een kwaliteitsaspect waarmee de medewerker voortdurend rekening moet houden gedurende werktijd.

Binnenkomend internet- en e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen, spam en soortgelijk ongerief. Mocht blijken dat een e-mailbericht een virus bevat, dan wordt het automatisch tegengehouden en worden de verzender en ontvanger daarover ingelicht. Indien desondanks materiaal wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger onverwijld contact op te nemen met de supportdesk ICT en het te melden als veiligheidsincident. De ontvanger onthoudt zich ervan om zelf verder enige actie te ondernemen, zodat verspreiding van het virus wordt voorkomen.

Het gebruik van internet- en e-mailverkeer kan door het Dijklander Ziekenhuis worden gemonitord. Deze registratie gebeurt om het beheer, de continuïteit, de veiligheid, de integriteit en de beschikbaarheid van de infrastructuur en de diensten te

waarborgen, verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan en om toezicht te houden op de naleving van de gedrags- en gebruiksregels binnen het ziekenhuis.

Gedragsregels gebruik werkstations

- Gevoelige bedrijfsinformatie en patiëntgegevens mogen uitsluitend op de netwerkschijf worden opgeslagen. Van deze, op de server geplaatste bestanden, maakt de ICT-afdeling volgens vastgestelde procedures back-ups.
- De medewerker die besluit bestanden op de lokale C-schijf op te slaan, is persoonlijk verantwoordelijk voor het beheer van deze bestanden. Van betreffende bestanden wordt door de afdeling ICT geen back-up gemaakt.
- De medewerker is zelf verantwoordelijk voor de inhoud van de door hem/haar zelf geproduceerde bestanden. Het ziekenhuis draagt geen verantwoordelijkheid.
- De medewerker dient de ter beschikking gestelde ICT-apparatuur te gebruiken conform de voorschriften en/of aanwijzigingen van medewerkers van de afdeling ICT.
- Apparatuur die onder verantwoording van ICT valt, mag alleen worden verplaatst door medewerkers van de afdeling ICT of door medewerkers na overleg en met toestemming van de supportdesk medewerker ICT.
- De medewerker mag de netwerkaansluitingen (kabels) niet zelf wijzigen.
- De medewerker dient aanwijzingen ten aanzien van beveiliging, zoals virusbestrijding, op te volgen.
- Incidenten die het normale gebruik van de voorzieningen verstoren dient de medewerker terstond aan de supportdesk ICT te melden.

Sancties (zie ook Procedure 'Sancties bij overtredingen inzake informatieveiligheid')

Bij handelen in strijd met deze gedragscode en de wet- en regelgeving met betrekking tot informatiebeveiliging (hierna: overtreding), kan het ziekenhuis (afhankelijk van de aard en de ernst van de overtreding) maatregelen treffen.
Hiervoor gelden de volgende stappen (vergelijkbaar met de stappen die we nemen in andere gevallen waarbij medewerkers afwijken van de gemaakte afspraken c.q. richtsnoeren e.d.):

Stap 1: De leidinggevende spreekt de medewerker aan op de verdenking van een overtreding en checkt de feiten en omstandigheden.
Stap 2: De leidinggevende stelt vast of een waarschuwing afgegeven wordt.
Stap 3: De leidinggevende stelt vast of andere disciplinaire maatregelen aan de orde zijn.

In algemene zin treedt het afdelingshoofd op als leidinggevende voor de medewerkers. De medisch specialist valt rechtstreeks onder de RvB, waarbij de medisch manager optreedt als eerste aanspreekpunt.
Dit betekent dat stap 1 wordt uitgevoerd door de medisch manager en de officiële disciplinaire stappen (2 en 3) door de RvB.

1. Aanspreken en onderzoek

Bij een mogelijke overtreding is het allereerst van belang te verifiëren of de gedragscode dan wel wet-/regelgeving met betrekking tot informatiebeveiliging daadwerkelijk is geschonden en/of zich een inbreuk op de informatiebeveiliging heeft voorgedaan.
De leidinggevende (afdelingshoofd of medisch manager) verzamelt hiervoor bewijsmateriaal. Vervolgens vindt hoor en wederhoor plaats met de medewerker waarbij de medewerker wordt aangesproken op de verdenking.
Indien aanwezig wordt hierbij het gevonden bewijsmateriaal besproken. Het gesprek dient in ieder geval inzicht te geven in de aard, ernst en omstandigheden van de overtreding.

Op ieder moment (voorafgaand of gedurende het onderzoek) kan de leidinggevende, besluiten de medewerker de toegang tot bepaalde ruimtes en informatie, digitaal en/of op papier, tijdelijk te ontzeggen. Hieronder valt dus ook de toegang tot computers en/of netwerken.

De leidinggevende kan bij het vermoeden van een ernstige overtreding, in overleg met HRM, de medewerker op non-actief stellen.

2. Waarschuwing

Indien uit het onderzoek blijkt dat er inderdaad sprake is van overtreding van de gedragscode en/of wet-/regelgeving zal in beginsel door de leidinggevende een officiële waarschuwing afgegeven worden, die schriftelijk wordt vastgelegd in het personeelsdossier.

3. Overige disciplinaire maatregelen

Afhankelijk van de aard, ernst en omstandigheden kan de schending arbeidsrechtelijke consequenties hebben, waaronder schorsing, berisping en het beëindigen van de arbeidsovereenkomst.
Overige disciplinaire maatregelen zijn het beëindiging van de samenwerkingsovereenkomst, het beëindigen van de uitzend-, detacherings- of dienstverleningsovereenkomst, het beëindigen van de vrijwilligersovereenkomst, het niet toelaten van de medewerker tot het ziekenhuis en de wettelijk verplichte aangifte bij politie (bijvoorbeeld bij het gebruik van kinderporno).

De leidinggevende beoordeelt, in overleg met het verantwoordelijke MT-lid en de HRM-adviseur, of een dergelijke maatregel aan de orde is. De RvB wordt door het verantwoordelijk MT-lid van deze maatregelen op de hoogte gesteld.

In uitzonderlijke gevallen (van zeer ernstige aard) kan overgegaan worden tot het onmiddellijk opzeggen van de arbeidsovereenkomst met een dringende reden, waarbij het vooraf geven van een waarschuwing achterwege kan blijven.

Bewustwording

Om te zorgen dat de gedragingen uit deze code onderdeel worden van het dagelijks handelen, is het van belang dat alle medewerkers op de hoogte zijn van de inhoud van de gedragscode en dient deze regelmatig onder de aandacht gebracht te worden.
Alleen dan wordt het onderdeel van het routinematig handelen en kunnen medewerkers elkaar aanspreken op ongewenst gedrag. Door de gedragscode informatieveiligheid met elkaar te bespreken, creëren we dat medewerkers de risico's begrijpen. Het stimuleren van het nemen van eigen verantwoordelijkheid staat hierbij centraal.

Nieuwe medewerkers (waaronder ook vrijwilligers, stagiaires en (vrijgevestigde) medisch specialisten), worden direct bij aanvang van hun werkzaamheden geïnformeerd over het informatiebeveiligingsbeleid en de verwachtingen van de organisatie hierover.
Hiertoe worden de volgende stappen gezet:

- Nieuwe medewerkers ontvangen bij de indiensttreding de brochure 'gedragscode Informatiebeveiliging & privacyreglement verwerking persoonsgegevens medewerkers Dijklander Ziekenhuis' als onderdeel van het indiensttredingspakket.
- Het afdelingshoofd/medisch manager zorgt er voor, al dan niet gedelegeerd aan de aangestelde 'buddy', dat de gedragscode bij aanvang van de werkzaamheden wordt besproken (zie deel A van het inwerkprogramma) en zorgt voor training on the job in het dagelijkse handelen met privacy gevoelige gegevens en het veilig gebruik van computer, internet en email.
- Het onderwerp Informatiebeveiliging maakt onderdeel uit van de Waterlanddag, de introductiedag voor nieuwe medewerkers.

Om het bewustzijn voor informatiebeveiliging niet te verliezen wordt het onderwerp regelmatig onder de aandacht gebracht bij de medewerkers.

- Het afdelingshoofd is verantwoordelijk om het onderwerp informatiebeveiliging en de verwachtingen van de organisatie hierover regelmatig onder de aandacht te brengen van hun medewerkers.
  Ditzelfde geldt voor de medisch manager die verantwoordelijk is voor de bewustwording op dit onderwerp van de leden van de vakgroep. Het afdelingshoofd en de medisch manager monitoren de situatie op de werkplek en maken onderwerpen die de informatiebeveiliging raken bespreekbaar.
  Zo wordt het beleid verduidelijkt, worden er werkafspraken gemaakt en verliest het onderwerp niet de aandacht op de afdeling. Indien gewenst kan de leidinggevende een medewerker aanstellen als ambassadeur voor informatiebeveiliging, die daarmee een voortrekkersrol op de afdeling vervult.
- In het najaar wordt de veiligheidsweek georganiseerd. Tijdens deze week wordt centraal aandacht gevraagd voor veiligheidsaspecten binnen het ziekenhuis, waarbij ook informatiebeveiliging aan de orde komt.
- Het initiatief hiervoor ligt bij de Adviseur Veilig en Vitaal Werken en de afdeling Communicatie, die de inhoud van de acties afstemmen met de Information Security Officer.
- Jaarlijks wordt rondom februari/maart het thema Informatiebeveiliging extra onder de aandacht gebracht binnen het ziekenhuis door middel van een campagne, e-learning, casuïstiek, tests, o.i.d.
  Het initiatief hiervoor ligt bij de Information Security Officer, die de uitvoering kan beleggen bij de Waterland Academie en/of de afdeling Communicatie (afhankelijk van de actie die wordt uitgezet).
  De information Security Officer zorgt dat de actie/opfristraining aansluit bij actuele thema's binnen het ziekenhuis.
  De acties hebben een verplicht karakter. Bij het uitzetten van de acties wordt getracht een zo groot mogelijk bereik te behalen gezien de verschillende groepen medewerkers binnen het ziekenhuis (waaronder bijv. uitzendkrachten, stagiaires, vrijwilligers, vrij gevestigden, medewerkers van externe partijen) en diversiteit aan werktijden.
  Voor het uitzetten van acties kan een beroep gedaan worden op de leidinggevenden dan wel de aangestelde ambassadeurs.

Slot

De medewerker stelt zich op de hoogte van deze gedragscode en de regels van het Dijklander Ziekenhuis ten aanzien van het ontvangen en bejegenen van bezoekers. In alle gevallen waarin deze gedragscode niet voorziet, beslist de raad van bestuur van het Dijklander Ziekenhuis

Inwerkingtreding

Deze gedragscodeis door de raad van bestuur vastgesteld op en in werking getreden met ingang van 13-12-2010.

Veiligheid: risicomomenten en te ondernemen acties

Het niet naleven van deze gedragscode kan o.a. schade berokkenen aan de privacy van de patiënt, o.a. resulterend in klachten en claims van patiënten, maatregelen van de IGZ, het verliezen van de NIAZ-accreditatie en imagoschade voor het Dijklander Ziekenhuis.
Daarnaast kan niet naleven van deze gedragscode leiden tot een verhoogd risico op uitval van informatiesystemen, met risico's voor de patiënt en de continuïteit van de bedrijfsvoering als gevolg.

Samenhangende documenten

Informatiebeveiligingsbeleid 2019-2024