BIJLAGE ARBEIDSREGLEMENT: Reglement inzake toegang tot elektronische gegevens in VZW Mariaziekenhuis

1 Toegang tot elektronische gegevens in VZW Mariaziekenhuis

De VZW Mariaziekenhuis maakt binnen nexuz health deel uit van het UZ Leuven netwerk. De algemene regels voor toegang tot elektronische gegevens van dit netwerk zijn daardoor ook van toepassing voor medewerkers van de VZW Mariaziekenhuis.

1.1 Gebruikersnaam en paswoord/wachtwoord

Om van start te gaan op het netwerk heb je een gebruikersnaam en een paswoord nodig:

- De **gebruikersnaam** (login of account) is uniek en wijzigt nooit.
- Het **paswoord** bepaal je zelf en is strikt persoonlijk (mag nooit worden doorgeven) . Om de 4 maanden dien je je wachtwoord te wijzigen.
- Nieuwe personeelsleden krijgen een login en paswoord op de eerste werkdag.
- Aanvraag van een gebruikersnaam en paswoord voor anderen dan personeelsleden (VZW Mariaziekenhuis medewerkers):
    - de aanvraag wordt gericht aan de dienst IT
    - nodige gegevens zijn: naam, voornaam, geboortedatum, geboorteplaats, rijksregisternummer en dienst(en) waartoe de medewerker toegang moet krijgen
    - de aanvraag gebeurt altijd door de verantwoordelijke van de dienst, per mail of brief (nooit mondeling of via telefoon).
- Met je gebruikersnaam en paswoord heb je standaard toegang tot je Windows werkomgeving, e-mail en standaard netwerkmappen.
- Toegang tot andere applicaties (KWS,...) en specifieke netwerkmappen dient apart te worden aangevraagd door de dienstverantwoordelijke (je krijgt deze niet automatisch als je een login aanvraagt). ***Indien voor toegang tot deze applicaties een aparte gebruikersnaam en paswoord is vereist, zijn deze strikt persoonlijk. Het is niet toegelaten om zich toegang te verschaffen tot deze applicaties door gebruik te maken van de gebruikersnaam en het paswoord van een andere gebruiker.***
- Bij het eerste gebruik dient het paswoord gewijzigd te worden.

1.2 Regels i.v.m. paswoorden

Paswoorden / wachtwoorden zorgen voor beveiliging en afscherming van gegevens en zijn dus ook van enorm belang. Om het voor een mogelijke "inbreker" niet te eenvoudig te maken om jouw paswoord te vinden, zijn deze aan een aantal regels onderworpen:

- Jouw wachtwoord moet **minimaal** 8 tekens lang zijn.
- Jouw wachtwoord moet verschillen van de 5 vorige wachtwoorden.
- **Het wachtwoord mag niet gelijk zijn aan jouw gebruikersnaam, of meer dan twee opeenvolgende karakters uit de gebruikersnaam bevatten**
- Je moet karakters gebruiken uit minstens ***3*** van de 4 volgende reeksen (Gebruik alleen karakters uit deze 4 reeksen):
    - Kleine letters abcdefghijklmnopqrstuvwxyz

  - Grote letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Nummers 0123456789
  - Andere Tekens ! " # $ % & ' ( ) * + ´ - . / : ; < = > ? @ [\ ] ^ _ `{ | } ~
- Vier opeenvolgende karakters mogen niet hetzelfde zijn
- Jouw wachtwoord wordt gecontroleerd aan de hand van een woordenboek:
  - Bestaande woorden van 4 tot 8 tekens mogen niet in je wachtwoord zitten.
  - We gebruiken Nederlandse, Franse, Engelse en Duitse woordenboeken.
  - Je mag woorden gebruiken waarvan je de klinkers vervangt door cijfers vb. waterval -> w8t3rv8l.
- **Iedereen is verantwoordelijk voor wat er onder zijn of haar login gebeurt. Een paswoord is persoonlijk en mag nooit worden doorgegeven of worden opgeschreven**. **Als je een toestel verlaat log je ook altijd uit.**
- **Men kan 7 foutieve pogingen ondernemen om een paswoord in te geven. Na de zevende poging zal uw gebruiker 30 minuten op inactief worden gezet.**
- Jouw paswoord moet om de 4 maanden gewijzigd worden. **Tussen twee wijzigingen moet je minstens 26 dagen laten.** Nadat het paswoord vervallen is, kan men dit nog gedurende 120 dagen wijzigen. Na deze periode wordt de login op inactief gezet. Enkel 'beheerders' kunnen de login terug activeren. Hierbij wordt automatisch een nieuw paswoord gecreëerd. De gebruiker wordt dan gevraagd dit paswoord opnieuw te wijzigen naar een persoonlijk paswoord.

1.3 Specifieke regels voor toegang vanuit andere omgevingen dan UZ Leuven

- Voor de Toegang tot het UZ Leuven netwerk en KWS binnen de (partner)ziekenhuizen dient authenticatie minstens op basis van 'something you know' te gebeuren (d.i. een voldoende sterk paswoord dat vervalt). Bij Single Sign On oplossingen dient hiermee rekening gehouden te worden (bijv. personeelsbadge 'something you have' EN paswoord 'something you know')
- Het paswoord moet voldoen aan dezelfde policies (of sterker) dan de paswoord policies van het KWS.
- Voor toegang tot het KWS van buiten het ziekenhuis (remote acces) dient de toegang te gebeuren met een extra vorm van 'strong authenticatie'. Er wordt niet alleen met KWS-login en paswoord ingelogd, maar ook steeds met een Token of E-id.
- De PC's waarop het KWS wordt uitgevoerd moeten uitgerust zijn met:
  - een recent antivirus programma
  - laatste security patches van microsoft

1.4 Creëren van logins

- Er worden enkel logins gemaakt voor fysieke personen die deze login strikt persoonlijk gebruiken. Er worden dus geen testlogins gemaakt die door meerdere personen gebruikt zouden kunnen worden.
- In specifieke omstandigheden kan een persoon een tweede login krijgen voor testdoeleinden (bv de leden van de implementatieploeg of developpers). Voor deze login gelden dezelfde strikte regels: enkel door die persoon te gebruiken, paswoord nooit doorgeven.

1.5 Distributie van paswoorden

- Paswoorden worden enkel individueel aan personen bezorgd. In het systeem is een tool voorzien om login en paswoord op een individueel blad te printen zodat dit aan de gebruiker kan gegeven worden.
- Nooit worden lijsten met paswoorden doorgegeven, aan prikborden gehangen, via mail doorgestuurd of op enige andere manier 'gepubliceerd' waardoor iemand paswoorden van andere gebruikers kan zien.

1.6 Gebruik van e-mail, intranet en internet

Het is essentieel dat elke gebruiker op het Inter- en intranet zijn/haar eigen verantwoordelijkheid ten aanzien van websites, systemen en personen draagt. De gebruiker is uiteindelijk zelf verantwoordelijk voor zijn/haar acties op het Inter- en intranet en bij gebruik van e-mail. (zie ook de tekst i.v.m. gebruik van email, intra- en internet, alsook de tekst i.v.m. discretieplicht).

2 Toegangscontrole in kws van nexuz health

2.1 Uitgangspunten

De VZW Mariaziekenhuis heeft gekozen voor 1 centraal dossier per patiënt over alle specialismen heen. Er werd bewust ook geen opsplitsing gemaakt tussen het verpleegkundig, het paramedisch en het medisch dossier. Indien men een patiënt behandelt krijgt men toegang tot het hele dossier voor de periode dat de behandeling duurt, uitgebreid met een 'grace period' waarop verder in dit document wordt ingezoemd. Dit moet de vlotte doorstroming van informatie ondersteunen en een multidisciplinaire aanpak bevorderen.

De KWS-software is dezelfde op alle plaatsen in de VZW Mariaziekenhuis: op elk werkstation zijn in principe alle functies beschikbaar.

Het is de toegangscontrole die bepaalt wie wat mag zien en wie welke acties mag uitvoeren.

2.2 Inloggen op KWS

Om toegang te krijgen tot KWS moet een persoon zich steeds aanmelden onder eigen login en paswoord.
Het ter beschikking stellen van de eigen gebruikersnaam en paswoord aan een andere persoon is niet toegelaten.

Alle acties en toegangen in KWS zijn gebaseerd op deze combinatie van login+paswoord. Regelgeving omtrent paswoorden is hierboven beschreven.

Op verschillende plaatsen in KWS wordt de login geregistreerd en kan men (laten) opvragen wie welke gegevens bekeken en/of gewijzigd heeft (steeds bij acties zoals het verzenden, corrigeren en vernietigen van gegevens en in verschillende gevallen bij het opvragen van gegevens).

Iedereen is persoonlijk verantwoordelijk voor de acties die onder zijn login in KWS worden uitgevoerd.

Een scherm kan om die reden ook eenvoudig beveiligd worden. Enkel de hieronder beschreven werkwijzen zijn toegelaten:

Schermbeveiliging: via de menu optie 'Algemeen' – 'Beveilig scherm' uit het mededelingenvenster of de shortcut 'ctrl+B'. Als je daarna als eerste terug inlogt krijg je alle vensters terug zoals ze achtergelaten zijn. Dit past men toe indien men kortstondig de toepassing op dat scherm verlaat. Logt een andere gebruiker in dan worden alle vensters in KWS gesloten. Indien een toestel 15 minuten niet gebruikt wordt dan gaat KWS automatisch in beveiliging.

Volledig uitloggen: via de menu optie 'Algemeen - Nieuwe gebruiker' of de shortcut 'ctrl+L'

Sessie doorgeven naar een ander werkstation: via de menu optie 'Sessie doorgeven' kunnen gebruikers van een zelfde discipline omloggen met behoud van openstaande vensters.

Uitbadgen

2.3 Toegangscontrole

De toegangscontrole in het KWS bestaat uit 2 luiken: de statische toegangscontrole en de dynamische toegangscontrole.

2.3.1 Statische toegangscontrole

De statische toegangscontrole controleert het verband tussen de (functie van) de gebruiker en bepaalde types gegevens of bewerkingen in het KWS:

> "Alleen artsen mogen medicatievoorschriften maken"
> "u mag verslagen valideren van het type X"

Meestal worden bewerkingen in het KWS gekoppeld aan functies ("arts", "verpleegkundige", "secretariaat", ...) maar ad hoc regels waar een bepaalde gebruiker een toegang krijgt tot een bepaalde actie zijn ook mogelijk. Men noemt deze vorm van toegangscontrole "statisch" omdat deze regels zelden wijzigen.

2.3.2 Dynamische toegangscontrole

De dynamische toegangscontrole in het KWS controleert het verband tussen een gebruiker en een patiënt. In principe heeft men geen toegang tot de patiënt tenzij men bij de behandeling betrokken is. Het KWS kan dit nooit met zekerheid weten maar probeert dit af te leiden. Hiervoor wordt een cascade van regels gebruikt.

Sommige van deze regels zijn erg voor de hand liggend:

> "als de patiënt bij deze gebruiker op consultatie komt"
> "deze gebruiker is als verpleegkundige verbonden aan eenheid X en de patiënt ligt op eenheid X" "er is een contact geregistreerd voor die patiënt waarvoor deze gebruiker assistent of supervisor is".

Andere zijn dan weer complexer:

> "de patiënt moet onderzoek X ondergaan, en u bent supervisor voor onderzoeken van het type Y waaronder onderzoek X valt"

Deze toegangen zijn dynamisch doordat de toegangen voortdurend veranderen in functie van de gegevens in het dossier. Doordat iemand een aanvraag doet of een afspraak boekt of ... krijgen de personen die hierop actie zullen uitvoeren automatisch toegang. Dit zijn meerdere duizenden wijzigingen per dag.

De cascade van regels die het KWS toepast om automatisch te bepalen of er toegang is tot het volledige dossier van de patiënt is zoals hieronder beschreven:

- De patiënt is nu aanwezig op spoedgevallen en de gebruiker is ook fysiek aanwezig op spoedgevallen
- De fysieke aanwezigheid van de gebruiker wordt bepaald door het ingelogd zijn op een *geregistreerd toestel* op de locatie spoedgevallen.
- De patiënt is (recent) aanwezig (geweest) op een eenheid en/of afdeling waar de gebruiker standaard toegang tot heeft
- De patiënt is (recent) aanwezig (geweest) op een eenheid waarvoor de gebruiker een uitzonderlijke toegang voor 1 dag/1 week heeft voor geactiveerd (i.f.v. wachten, dynamisch inzetten vpl op andere eenheden, ...)

- De gebruiker heeft nog een openstaand contact aan hem toegewezen voor deze patiënt
- De gebruiker was toegewezen aan of was de validator (of *geen verslag nodig*) van een contact dat nog geen 14 maanden is afgesloten. (zie grace period)
- De gebruiker hoort tot een functiemeting waarvoor deze patiënt een geplande aanvraag heeft openstaan
- De gebruiker heeft toegang via zeer specifieke regels voor my nexuz pro gebruikers, externe gebruikers, …

Daarnaast kan een gebruiker ook nog toegang hebben tot een specifiek resultaat (zonder toegang tot het volledige dossier) op basis van zijn postbus en/of de afdruklijst.

Grace period

De dynamische toegang dooft uit na een periode die afhangt van de reden waarom men toegang kreeg. Het is niet zo dat men onbeperkt toegang krijgt tot het *gehele* dossier van een patiënt. Men heeft wel onbeperkt toegang tot het deel van de eigen afdeling, maar toegang tot andere delen van het dossier valt 'na een tijd' weg. Zodra de patiënt weer een behandelrelatie heeft met de gebruiker krijgt deze weer toegang tot het hele dossier.

2.3.3 Overrules

Er is een structureel probleem met de implementatie van elke dynamische toegangscontrole: ze is steeds gebaseerd op reeds geregistreerde gegevens (bv de aanwezigheid van de patiënt). Soms is echter toegang nodig op basis van intentie:

> "de patiënt zal bij mij op consultatie komen"
> "de patiënt zal door mij geanesthesieerd worden", ...

Ook in geval van nood moet iemand het dossier kunnen openen, zelfs al heeft het KWS geen gegevens waaruit het een behandelrelatie kan afleiden (naast overrule op één dossier bestaat zo ook overrule voor 1 dag of één week waarmee artsen of verpleegkundigen toegang kunnen krijgen tot alle patiënten van een eenheid of afdeling. Deze mogelijkheid is specifiek voorzien voor wachtdiensten bij artsen of onverwachte vervangingen bij verpleging).

In dergelijk gevallen is een overrule mogelijk: het KWS vraagt een reden en geeft daarna toegang, maar:

- Alleen de dynamische toegangscontrole wordt overruled. Men krijgt toegang tot de patiënt maar nog steeds met de rechten gekoppeld aan de eigen functie. M.a.w. een verpleegkundige blijft voor het systeem een verpleegkundige, een arts blijft een arts.
- Alle acties die men doet in dat dossier worden in hoge mate van detail gelogd. Het is achteraf perfect controleerbaar wat iemand gezien of gedaan heeft.
- De personen die als supervisor voor een patiënt verantwoordelijk zijn krijgen de lijst met overrules te zien telkens zij een dossier van een van hun patiënten openen. Als ze hierop klikken krijgen ze de details in de log te zien. Indien zij onregelmatigheden vermoeden, kunnen zij dit via de KWS-implementatieploeg naar de hoofdgeneesheer doorgespelen.

2.3.4 In bescherming nemen van patiënten en verslagen

Om de dossiers van sommige patiënten beter te beschermen is het mogelijk om een patiënt in bescherming te nemen. De gebruiker die gegevens van een beschermde patiënt raadpleegt merkt niets speciaal. Er wordt enkel in een log bijgehouden dat hij/zij toegang heeft gevraagd tot de patiënt én alle acties worden gelogd.

Indien een patiënt in bescherming moet genomen worden dan verwittigt men de KWS-implementatieploeg.

Medewerkers van de VZW Mariaziekenhuis zijn standaard 'beschermde patiënten'.

2.3.5 Log voor bevoegde personen

Supervisoren en bevoegde personen kunnen **gelogde toegangen** (oa overrules) op een patiëntdossier rechtstreeks opvragen **via het dossier** zelf. Bovenaan links op het patiëntdossier staat naast het 'slotje' voor 'volledige toegang' een **knopje** om de lijst met gelogde toegangen op te vragen.

De supervisor kan de gegeven redenen nakijken en indien nodig maatregelen treffen. Elke supervisor beschikt ook over de stored query ToegewezenOverrules die voor alle patiënten waaraan hij is toegewezen een overzicht geeft van de bovenstaande doorbrekingen en bijhorende redenen. Deze query is eveneens oproepbaar via het menu "Werklijsten" optie "Overzicht overrules"

Elke gebruiker (of patiënt) kan via zijn behandelende arts een overzicht krijgen van de bovenstaande doorbrekingen en bijhorende redenen voor zijn eigen patiëntendossier.

2.3.6 Vertrouwelijke en beschermde rapporten

Specifieke laborapporten worden automatisch als confidentieel beschouwd. Het betreft ondermeer HIV en bepaalde cytologische onderzoeken. Deze uitslagen zijn enkel beschikbaar voor de aanvragers en voor supervisoren en artsen waarvoor een open contact van de betrokken patiënt bestaat.

Verslagen van de dienst Menselijke Erfelijkheid, Psychiatrie en Sociaal Werk kunnen "beschermd" worden. Ze zijn dan enkel beschikbaar binnen deze dienst en voor de contactbestemmelingen van dat verslag. Dit is voor deze diensten beschikbaar omdat hun verslaggeving door de aard van de dienst vaak gegevens van 'derden' bevat.

2.3.7 Meta-toegangscontrole

De toegangen van de gebruikers worden onderhouden door gebruikers met meta-toegangscontrole. Deze gebruikers hebben de mogelijkheid hun toegangen tot eenheden en/ of afdelingen door te geven of af te nemen van andere gebruikers. Ze beschikken over een overzichtslijst van alle gebruikers die toegang hebben tot hun eenheden en/of afdelingen.

Toegang tot KWS wordt enkel gegeven aan wie het KWS nodig heeft voor zijn/haar functie binnen het ziekenhuis. In principe staat een persoon die toegang heeft tot KWS onder contract: personeelscontract van de VZW Mariaziekenhuis of partnerziekenhuis, contract als arts met het ziekenhuis, of een individueel contract met het ziekenhuis voor onderzoekers, tijdelijke medewerkers, medewerkers in dienst van artsen.

Anderen zijn (co) assistenten en stagiairs , stage verpleging... waarbij uitgegaan wordt van een verbintenis met de onderwijsinstelling.

In alle andere gevallen dient de toegang tot KWS overlegd te worden met de KWS implementatieploeg die oa op basis van de vraag toegang tot KWS kan afwegen.

Het zetten van toegangen is gebonden aan regels. Hierbij dient steeds de wettelijkheid gerespecteerd. Bv een secretaresse mag geen toegang krijgen als supervisor (die een arts is) waardoor zij (of hij) verslagen zou kunnen valideren of medicatie voorschrijven. Het diploma van de betrokkene kan hier dus belang hebben. Toegangen dienen ook altijd zo beperkt mogelijk te zijn: wat men nodig heeft in functie van de patiëntengroep en de eigen taakinhoud, maar wel *enkel wat men nodig heeft*.

In elk geval zal ieder die KWS-toegangen beheert dit doen volgens de regels en procedures die binnen UZ Leuven gelden. Als aanpassingen aan deze regels nodig zijn gebeurt dat in gezamenlijk overleg met de partnerziekenhuizen zodat voor het ganse systeem steeds dezelfde regels gelden. UZ Leuven blijft hierbij wel de hoofdbeheerder.

3 Toegang tot beheersmodules van kws

In de samenwerking met de partnerziekenhuizen is het een basisprincipe dat de partners hun eigen configuraties onderhouden en hun eigen basisgegevens beheren.

Dit gaat o.a. over

- BAS waarin alle afdelingscodes, eenheden en artsen staan
- toegangsbeheer: maken en beheren van logins
- toegangscontrole in KWS
- opnamebeheer
- beheer zorgmodule
- beheer van de OKA planner (beheer van OKA zalen, OKA tijd etc...)
- beheer van afsprakenboeken
- beheer van de MZG toepassing voor het eigen ZH
- Magister
- KWS beheer (voor de KWS implementatie ploegen)
- ...

In al deze situaties zullen specifieke medewerkers van de partnerziekenhuizen toegang krijgen tot configuratietools in KWS, BAS of een andere toepassing. Hierdoor hebben zij echter ook toegang tot deze gegevens van UZ Leuven en de andere partners (m.a.w. medewerkers van de partnerziekenhuizen zullen bv de UZ Leuven bestanden kunnen aanpassen. Afspraak is uiteraard dat niet te doen, maar er zijn geen harde 'muren' die de gegevens van de ziekenhuizen hier scheiden).

Vandaar volgende afspraken voor iedereen die toegang nodig heeft tot een configuratietool:

- zij volgen voor die specifieke tool een opleiding + stage bij de UZ Leuven verantwoordelijke zoals een UZ Leuven medewerker die zou krijgen
- de UZ Leuven verantwoordelijke voor die tool evalueert de kunde en kennis van die medewerker en beslist over zijn bekwaamheid om op een bepaald moment zelfstandig aanpassingen te mogen doen. In extremis betekent dit dat UZ Leuven kan beslissen iemand geen toegang te geven (zelfde als na een proefperiode van een UZ Leuven medewerker).
- medewerkers van de partnerziekenhuizen die met een bepaalde tool werken, vormen een team over de ziekenhuizen heen:
    - zij werken volgens dezelfde regels en procedures, UZ Leuven is hoofdbeheerder.
    - aanpassingen worden samen overlegd
    - zij staan elkaar bij in raad en daad
    - zij hebben regelmatig overleg

BIJLAGE: Gedragscode betreffende het gebruik en de controle van e-mail, intra- en internet

1. Doelstelling

Deze gedragscode heeft tot doel om:

- de veiligheid, betrouwbaarheid en bescherming van de persoonlijke levenssfeer te waarborgen binnen de systemen en netwerken van de VZW Mariaziekenhuis en de netwerken en systemen van derden
- de goede naam van de VZW Mariaziekenhuis als verantwoord internetgebruiker te waarborgen
- de dienstverlening op het netwerk niet te verstoren
- de persoonlijke levenssfeer en veiligheid van de individuele gebruikers te beschermen
- de rechten en plichten van de gebruikers van het internet-, intranet- en e-mailsysteem van de VZW Mariaziekenhuis te bepalen

2. Toepassingsgebied

Deze gedragscode is van toepassing op alle personen die toegang wordt verleend tot de computersystemen van de VZW Mariaziekenhuis en van daaruit gebruik maken van onderstaande systemen (verder 'de systemen' genoemd):

- e-mail
- internet
- intranet

3. Verantwoordelijkheid

Het leidinggevend personeel en de systeembeheerders zullen erop toezien dat de gebruikers de bepalingen van deze gedragscode naleven. De specifieke rechten en plichten van de systeembeheerders maken het voorwerp uit van een afzonderlijk document.

De onderstaande bepalingen met betrekking tot het toegelaten en niet-toegelaten gebruik zijn niet limitatief. Indien een gebruiker zekerheid wenst met betrekking tot de toelaatbaarheid van bepaalde acties, kan hij/zij contact opnemen met zijn/haar leidinggevende.

4. Geautoriseerde toegang

a. Gebruikerstoegang

Om toegang te hebben tot de computersystemen van de VZW Mariaziekenhuis wordt de gebruiker een loginnaam toegekend door de dienst IT. De toegang wordt pas verleend na het ondertekenen van de arbeidsovereenkomst.

b. Paswoord

Iedere gebruiker dient zijn login te beschermen met een sterk paswoord. De minimale vereisten van dit paswoord worden beschreven in het 'Reglement inzake toegang tot elektronische gegevens in de VZW Mariaziekenhuis'. Dit paswoord is strikt vertrouwelijk en mag niet aan anderen doorgegeven worden. Iedere gebruiker is dan ook verantwoordelijk voor wat onder zijn/haar paswoord binnen de systemen gebeurt. Er worden geen gemeenschappelijke logins aangemaakt.

5. Gebruik van de systemen

a. Rechtmatig en verantwoord gebruik

De gebruiker is gemachtigd om de systemen te gebruiken voor opdrachten die ressorteren onder de doelstellingen van de VZW Mariaziekenhuis, in zoverre dit de ondersteuning van de klinische activiteit van de VZW Mariaziekenhuis niet verstoort.

Een mznl-mailadres dient uitsluitend voor professioneel gebruik. Alle berichten die vanuit dit mailadres worden verzonden, worden beschouwd als professionele e-mail.

Persoonlijk gebruik van de systemen is enkel toegelaten in noodgevallen en in zoverre dit op geen enkele wijze de arbeidsprestaties in het gedrang brengt.

De leden van de overlegorganen en de leden van de syndicale afvaardiging mogen vertrouwelijk gebruik maken van de systemen in functie van hun mandaat.

Controle en bescherming van de privacy

Bij de uitgevoerde controles zal de VZW Mariaziekenhuis steeds streven naar een evenwicht tussen het respect voor de privacy van de gebruiker en het recht op een normaal werkgeverstoezicht door de VZW Mariaziekenhuis.

De controles zullen gericht zijn op het vaststellen en tegengaan van misbruiken, het nagaan van de goede werking van het netwerk en de systemen en het garanderen van de goede uitvoering van de telecommunicatie. Deze gerichte controles gebeuren door de registratie van 'logs', d.i. door het registreren naar welk netwerkadres een webpagina verzonden wordt, of tussen welke e-mailadressen een bericht uitgewisseld wordt.

Deze registratie is een verwerking van persoonsgegevens die valt onder de Wet tot bescherming van de persoonlijke levenssfeer. De bepalingen van deze wet zijn dan ook op deze registratie van toepassing.

b. Niet toegelaten gebruik

De onderstaande bepalingen zijn niet limitatief. Indien een gebruiker zekerheid wenst met betrekking tot de toelaatbaarheid van bepaalde acties, kan hij/zij contact opnemen met het diensthoofd.

Verstorend gebruik: het gebruik van de systemen dat een inmenging in het werk van anderen vormt, het ongeautoriseerd verwijderen of wijzigen van andermans bestanden, overdadig gebruik van de systemen of de voedingsbronnen van de systemen, ...

Onwettig gebruik: het verkrijgen of onrechtmatig verkrijgen van toegang tot het ***intranet of hierop beschikbare toepassingen of*** het internet door gebruik te maken van enig toegangscontrolemechanisme dat aan een andere gebruiker toegewezen werd, het beschikbaar stellen van het persoonlijke toegangscontrolemechanisme tot het Internet aan personen die niet behoren tot de rechtmatige gebruikersgroep van de VZW Mariaziekenhuis, zich ongeautoriseerd toegang verschaffen of pogen te verschaffen tot enige computer, computernetwerken, gegevensbestanden, gegevens of elektronisch opgeslagen informatie, het downloaden van het internet en/of het doorsturen via e-mail van illegale software of software afkomstig van een onbetrouwbare bron,...

Aanstootgevende of beledigende gegevens: het verkrijgen, verzenden, opzoeken, weergeven, uitprinten, of anderszins verspreiden van gegevens die redelijkerwijze anderen beledigen, bedreigen of in verlegenheid brengen, of die seksueel expliciet, frauduleus of anderszins ongepast zijn in een professionele omgeving. Het versturen van uitspraken, taal, beelden of andere documenten die

redelijkerwijze aanzien worden als beledigend of vernederend voor anderen op basis van ras, nationaliteit, geslacht, seksuele geaardheid, leeftijd, handicap, religie of politieke overtuiging.

Intellectuele eigendom: de gebruikers dienen de bepalingen van de wetgeving inzake intellectuele eigendomsrechten na te leven.

Gevoelige gegevens van de VZW Mariaziekenhuis: gegevens kunnen 'openbaar', 'intern', 'vertrouwelijk' of 'strikt persoonlijk en vertrouwelijk' zijn. Omwille van de bewijswaarde en het geringe confidentiële karakter is e-mail echter niet geschikt voor het doorsturen van vertrouwelijke en belangrijke communicatie (bv. medische gegevens), tenzij door medewerking van de dienst informatica maximale geheimhouding is verzekerd. Bij het e-mailgebruik moet men bovendien rekening houden met het feit dat het e-mailbericht altijd ergens kan bewaard worden, ook na de verwijdering ervan door de gebruiker.
De gebruiker dient dan ook de systemen slechts te gebruiken indien deze aangewezen zijn voor de bedoelde communicatie. Zo nodig dient gevoelige communicatie op de gepaste manier gelabeld ('vertrouwelijk',...) te worden.

6. Beheer van de systemen

a. Beheer van de opgeslagen gegevens

Op de centrale fileserver wordt dagelijks een back-up gemaakt van de gegevens op de persoonlijke netwerkschijf van de gebruiker. De VZW Mariaziekenhuis is niet verantwoordelijk voor backup van lokaal opgeslagen bestanden.

Wanneer een gebruiker minstens 1 jaar uit dienst is, worden zijn/haar persoonlijke niet-actieve bestanden verwijderd.

b. Controle door de werkgever

De VZW Mariaziekenhuis zal zich enkel toegang verschaffen tot de harde schijf van de gebruiker of tot de persoonlijke data van de gebruiker op de fileservers mits diens toestemming of indien problemen die de werking van het algemene systeem in gevaar brengen (waaronder virussen), worden vastgesteld.

De gebruiker stemt er in het bijzonder mee in dat de VZW Mariaziekenhuis binnen de perken van het normaal werkgeverstoezicht het internet-, intranetgebruik en de e-mailcommunicatie controleert.

De controles zijn gericht op het vaststellen en tegengaan van misbruiken, het nagaan van de goede werking van het netwerk en de systemen en het garanderen van de goede uitvoering van de telecommunicatie.

c. Bescherming tegen virussen

De systemen worden door een centraal en een lokaal anti-virusprogramma gecontroleerd. Enkel indien het lokaal anti-virusprogramma het virus eerst detecteert, zal de gebruiker hierover een waarschuwing ontvangen.

In beide gevallen wordt er centraal vanuit de dienst informatica ingegrepen en zullen de data aangetast door het virus indien mogelijk gedesinfecteerd, zoniet verwijderd worden.

d. Veiligheid

Elke gebruiker dient bij het verlaten van de werkplek, zelfs voor en korte periode, de nodige maatregelen te nemen om toegang tot de persoonlijke account door derden te vermijden.

De systeembeheerders hebben de plicht alle nodige maatregelen te nemen om de goede werking van de computersystemen van de VZW Mariaziekenhuis te garanderen, waarbij absolute prioriteit moet verleend worden aan de ondersteuning van de klinische activiteit.

In het kader hiervan kunnen gebruikers tijdelijk, in afwachting van een beslissing door de Directie of de Medische Raad, en ook preventief, volledig geweerd worden van de computersystemen van de VZW Mariaziekenhuis.

7. Inbreuken op de gedragscode

a. Procedure voor rapportering van inbreuken

De VZW Mariaziekenhuis doet een beroep op de verantwoordelijkheidszin van iedere gebruiker om zich te houden aan de bepalingen van deze gedragscode.

Ingeval een gebruiker kennis krijgt van een inbreuk, dient hij/zij dit te melden via de leidinggevende.

Iedere gebruiker heeft bovendien de plicht om via de leidinggevende de VZW Mariaziekenhuis te informeren indien hij/zij methoden te weten komt die de beveiliging of de privacy van de gegevens in het gedrang brengen.

b. Sancties

In geval een inbreuk op de bepalingen van deze gedragscode wordt vastgesteld, zijn de volgende sancties van toepassing:

- Tijdelijke of definitieve herroeping van de autorisatie tot het gebruik van het Internet en/of het e-mailsysteem in het bijzonder.
- Een sanctie zoals voorzien in art. 52 van het Arbeidsreglement van de VZW Mariaziekenhuis.
- In zwaarwichtige gevallen: ontslag (arbeidsreglement, art 57)
- Verbod van toegang tot de gebouwen van de VZW Mariaziekenhuis (enkel voor gasten)

De personeelsdirecteur en/of de directie zal in overleg met het betrokken diensthoofd bepalen welke sanctie zal opgelegd worden. De sanctie wordt in het persoonlijk dossier van de werknemer genoteerd.

Voor gasten van de VZW Mariaziekenhuis zal de juridische werkgever op de hoogte gesteld worden van de inbreuk en de eventuele tijdelijke of definitieve herroeping van de autorisatie.

De gebruiker kan tegen het opleggen van de sanctie schriftelijk beroep aantekenen bij de Algemeen Directeur van de VZW Mariaziekenhuis.

Sommige inbreuken maken bovendien het voorwerp uit van een strafrechtelijke bepaling en kunnen bijgevolg aanleiding geven tot gerechtelijke vervolging.

BIJLAGE : Discretieplicht binnen de VZW Mariaziekenhuis

De discretieplicht omvat het geheel spelregels (deontologisch, ethisch, …) die dienen gerespecteerd te worden door medewerkers, aangestelden en werknemers van de VZW Mariaziekenhuis, zowel zelfstandigen, werknemers als vrijwilligers (verder medewerkers van de VZW Mariaziekenhuis genoemd), bij het omgaan met medische en niet-medische gegevens over patiënten, collega's, bezoekers, … Het respect voor de discretieplicht gaat ruimer dan alleen het respect voor het medisch beroepsgeheim of de privacywetgeving. Voor de inhoud van het medisch beroepsgeheim sensu stricto verwijzen wij naar de specifieke reglementeringen ter zake (o.a. art. 458 Strafwetboek, Art 50 van het arbeidsreglement).

1. Algemeen en absoluut karakter van de discretieplicht

Een strikt respect voor de discretieplicht is een fundamenteel principe voor alle medewerkers van de VZW Mariaziekenhuis. Het betreft hier niet alleen de medewerkers die rechtstreeks met de patiëntenzorg verbonden zijn, doch ook dezen die niet rechtstreeks met de zorg verbonden zijn en al diegenen die zich in het kader van hun beroepsuitoefening of hun opleiding binnen de VZW Mariaziekenhuis bewegen. Ook personen die in dienst van of aangesteld door zelfstandige artsen in contact komen met patiënten of gegevens van patiënten van de VZW Mariaziekenhuis zijn aan discretieplicht onderworpen.

De risico's om de discretieplicht te overtreden zijn geëvolueerd, o.m. door het inschakelen van de computer in het zorggebeuren. De draagkracht van de discretieplicht in het dagelijks werk dient continu onder de aandacht te blijven.

2. Inhoud van de discretieplicht

De discretieplicht respecteren betekent dat u de informatie die u krachtens uw beroep weet, geheimhoudt.

De discretieplicht heeft in het algemeen betrekking op alles wat u als medewerker van het de VZW Mariaziekenhuis ziet, hoort, verneemt, vaststelt, ontdekt of opvangt tijdens of in het kader van de uitoefening van uw beroep. Het gaat hierbij niet alleen om gegevens van medische aard, doch tevens over alle andere inlichtingen van vertrouwelijke aard.

De discretieplicht respecteren is niet eenvoudig: De 'spelregels' zijn immers niet sluitend bepaald.

Daarenboven is men niet steeds voorbereid op hoe te reageren op vragen van anderen. Of vraagt men zich bij zijn dagdagelijkse gedragingen niet altijd meer af of iets wel mag. Of denkt men dat men informatie mag doorgeven omdat de ontvanger ook door de discretieplicht gebonden is. Of is men te vlug overtuigd dat de praktische werkbaarheid toch wel dient te primeren.

Huidige bepalingen beogen dan ook een leidraad te zijn bij het omgaan met informatie over patiënten en over andere medewerkers van de VZW Mariaziekenhuis uit respect voor de privacy waarop zij recht hebben. Iedere patiënt en ieder personeelslid moet er immers op kunnen rekenen dat gegevens die verband houden met zijn aanwezigheid of beroepsuitoefening in de VZW Mariaziekenhuis als vertrouwelijk worden beschouwd.

3. Enkele concrete situaties

Hieronder enkele 'spelregels' m.b.t. het respecteren van de discretieplicht in een aantal herkenbare situaties:

- U kan enkel inzage nemen van een patiëntendossier of gegevens uit het patiëntendossier onder welke vorm ook, mits toestemming van de verantwoordelijke arts en in zoverre dit nodig is voor de zorgverlening. De toestemming van de verantwoordelijke arts kan ook

globaal (d.w.z. niet geïndividualiseerd per patiënt) of impliciet zijn (af te leiden uit de opdracht), tenzij hierover andersluidende afspraken werden gemaakt.

- U bent niet gerechtigd om op louter eigen initiatief gegevens in uw persoonlijk medisch dossier of personeelsdossier te raadplegen. De Wet op de patiëntenrechten en de privacywetgeving kennen u welbepaalde rechten toe (recht op het vragen van inzage en eventueel afschrift, recht op mededeling), doch kent u geen onmiddellijk rechtstreeks inzagerecht toe. Er bestaan hieromtrent welomschreven procedures.
- De arts die m.b.t. zichzelf of zijn familieleden optreedt als (mede)behandelende arts en als dusdanig bekend gemaakt werd, heeft uiteraard wel een rechtstreeks inzagerecht in de betreffende medische gegevens.
- Medische secretariaten en archiefruimten zijn in principe niet toegankelijk voor personen die bij de concrete dienstverlening van die diensten niet betrokken zijn.
- Met uitzondering van de informatie die u beroepshalve moet verstrekken en tenzij de patiënt duidelijk door één of andere reactie of na bevraging te kennen heeft gegeven dat men van deze zwijgplicht is ontslagen: (*M.b.t. het medisch beroepsgeheim geldt dat de patiënt de arts in een aantal gevallen op eigen aangeven van zijn zwijgplicht kan ontheffen, doch de arts is niet verplicht om daar op in te gaan.*)
    - mag u geen enkele mededeling doen omtrent namen van patiënten die u heeft behandeld of van wie u weet dat ze in het ziekenhuis zijn, zullen komen, of geweest zijn, noch betreffende de dienst waar of de aandoening waarvoor zij verzorgd worden. Dit geldt zowel intern (binnen de eigen afdeling), als extern (buiten de eigen afdeling of buiten de VZW Mariaziekenhuis) en dit zowel ten aanzien van collega's als ten aanzien van andere patiënten, familie, vrienden, enz.
      Bovendien geldt dit in principe ook bij een politie- of een gerechtelijk onderzoek. Het algemeen geldende principe is hier dat de behandelende arts (of zijn vervanger) deze instanties te woord staat. Alle andere medewerkers verwijzen naar hen door.
      Indien medische informatie binnen een (multidisciplinaire) groep moet gedeeld worden om een goede behandeling mogelijk te maken, moet dit op een correcte manier gebeuren, met eerbied voor de privacy en de waardigheid van de patiënt en waarbij overbodige details achterwege worden gelaten.
      Er weze tenslotte opgemerkt dat deze bepalingen uiteraard evenzeer gelden ten aanzien van werknemers die niet rechtstreeks in de zorgverlening ingeschakeld zijn, doch die tijdens of in het kader van de uitoefening van hun functie in de VZW Mariaziekenhuis (medische) informatie vernemen (bv. medewerkers Medische Administratie, Inschrijvingen).
    - mag u inlichtingen per telefoon slechts verstrekken indien u zeker is van de identiteit van uw gesprekspartner, deze persoon recht heeft op die informatie (bv. ouders) of bij de behandeling of de nazorg betrokken is (bv. huisarts), én op voorwaarde dat de verantwoordelijke arts hiermee akkoord gaat.
- Het enkel uit nieuwsgierigheid of sensatiezucht bespreken van vertrouwelijke (medische) informatie over bekende personen, politieke personaliteiten, artiesten, sportlui, artsen, medestudenten, personen werkzaam in het ziekenhuis, enz. is een grove inbreuk op de discretieplicht. Dit blijft eveneens van toepassing wanneer deze persoon is overleden.
- Indien u iemand ontmoet die u kent, kan u uiteraard deze persoon begroeten, doch zonder verder in gesprek te gaan m.b.t. diens aanwezigheid in de VZW Mariaziekenhuis, tenzij deze persoon zelf hiertoe het initiatief neemt.
- U dient er steeds over te waken dat u met collega's geen gegevens m.b.t. patiënten bespreekt of met de patiënt zelf geen vertrouwelijke gegevens over zijn toestand uitwisselt of opvraagt in ruimten waar u het risico loopt dat anderen kunnen meeluisteren (bv. cafetaria, kleedkamer, gang, wachtzaal, liften, bushalte). Indien dit door omstandigheden niet uitgesloten kan worden (bv. niet-verplaatsbare patiënten in gemeenschappelijke patiëntenkamer), dient u er voor te zorgen dat u de privacy van de patiënt maximaal respecteert (bv. met gedempte stem spreken, enz.).
- Omwille van het geringe confidentiële karakter is e-mail niet geschikt voor het intern of extern doorsturen van vertrouwelijke en belangrijke communicatie zoals bv. medische gegevens.

- Let er steeds op dat u geen documenten waarmee anderen gegevens i.v.m. patiënten kunnen achterhalen achteloos laat rondslingeren (bv. kladblaadjes op nachtkastjes of in kleedkamers).
- Klinische ervaringen kunnen, buiten het kader van de behandeling, enkel met collega's uitgewisseld worden op voorwaarde dat de besproken patiënt op geen enkele wijze herkenbaar is en het gesprek niet plaatsvindt in een openbare ruimte.
- Medische dossiers kunnen in het kader van een wetenschappelijke studie worden geraadpleegd voor zover dit onderzoek geschiedt onder toezicht van een arts en mits schriftelijk akkoord van een vast staflid van de dienst waartoe het dossier behoort, indien het medisch geheim niet wordt geschonden en de procedure conform is met de wetgeving betreffende de rechten van de patiënt.
- Inlichtingen over personeelsgegevens (bv. adres- of loongegevens) of andere gegevens (bv. dienstorganisatie, individuele uurroosters) mag u enkel meedelen conform de bepalingen van de wetgeving op de privacy.
- Niet-publieke informatie over de VZW Mariaziekenhuis (gegevens over de financiële situatie, statistische gegevens, enz.) waarvan u kennis krijgt tijdens of in het kader van de uitoefening van uw functie bij de VZW Mariaziekenhuis, kan u enkel meedelen aan diegenen waaraan u dit gerechtigd bent te doen en in zoverre u deze informatie beroepshalve moet verstrekken.

4. Discretieplicht en het gebruik van computersystemen in de VZW Mariaziekenhuis

Heel wat gegevens waarop de discretieplicht van toepassing is, werden geïntegreerd in geïnformatiseerde bestanden. De toegang tot deze systemen is geregeld via een systeem van toegangscontrole, wat de VZW Mariaziekenhuis toelaat om de toegang te beperken tot de medewerkers van de VZW Mariaziekenhuis die deze informatie voor beroepsdoeleinden nodig hebben. Waar mogelijk en werkbaar, werden ook technische toegangsbeperkingen en -controles ingelast.

U begaat een inbreuk op de regels van de discretieplicht wanneer men de computersystemen van de VZW Mariaziekenhuis gebruikt om:

- gegevens op te vragen die u niet nodig heeft
- programmacodes te achterhalen en te gebruiken die niet voor u zijn vrijgegeven
- de u gekende codes/paswoorden door te geven (*Paswoorden van login-namen mogen nooit doorgegeven worden. Paswoorden van gemeenschappelijke login-namen mogen enkel aan bevoegden worden meegedeeld.*)
- computerlijsten, etiketten of afdrukken met patiënten- of personeelsgegevens te laten rondslingeren of buitenshuis te verspreiden (bv. als klad- of tekenpapier)

Het Reglement inzake de toegang tot het Klinisch Werkstation regelt de toegang tot en het gebruik van het KWS. Enkele belangrijke aandachtspunten hierbij zijn:

- **Van eenieder wordt verwacht dat hij uitsluitend informatie opzoekt om gevestigde professionele redenen**. Het opzoeken van andere informatie (bv. eigen medische gegevens of deze van familieleden wanneer men niet optreedt als (mede-)behandelende arts, administratieve gegevens zoals data van afspraken of consultaties, kamernummer in functie van een privébezoek), het gebruik van de login of het codewoord van een andere persoon of het inkijken van een "openstaand patiëntencontact" wordt als een ernstige schending van de privacy en de discretieplicht beschouwd.
- De toegang tot KWS is geregeld via afgebakende gebruikerstoegangen. Om redenen van praktische en vlotte werkbaarheid is het technisch steeds mogelijk om een toegangsbeperking te doorbreken. Het respect voor de discretieplicht geldt echter ten allen tijde: een toegangsbeperking mag dan ook enkel om welbepaalde gerechtvaardigde redenen doorbroken worden.

- Indien u over een login en codewoord beschikt dat u toegang verleent tot het KWS, dient u dit geheim te houden. Indien u wenst dat één van uw medewerkers ook rechtsreeks toegang heeft tot bepaalde gegevens van het KWS waartoe u zelf gerechtigd bent, bent u niet geoorloofd om uw login en codewoord door te geven. Iedereen is immers persoonlijk verantwoordelijk voor de acties die onder zijn login in het KWS worden uitgevoerd. Indien nodig kan een gemotiveerde aanvraag gericht worden t.a.v. van de KWS-implementatieploeg teneinde een aparte login met afgebakende toegangsmogelijkheden voor uw medewerker te voorzien.
- Wanneer u in KWS werkt, dient u de "openstaande dossiers" tot een minimum te beperken en zeker nooit onbewaakt te laten. Gebruik dan ook "Beveilig scherm" (CRTL-B) uit het menu "Algemeen" om het KWS af te sluiten voor onbevoegde blikken wanneer u uw computer verlaat.
- Patiënten die hierom verzoeken kunnen als "beschermde patiënt" worden aangeduid in het KWS. Dit betekent dat elke toegang tot hun elektronisch dossier gelogd wordt, wat een controle van alle acties in hun dossier mogelijk maakt. Als personeelslid van de VZW Mariaziekenhuis wordt u automatisch als "beschermde patiënt" in het KWS aangeduid.
- Iedereen die vermoedt dat onbevoegden zich via het KWS toegang verschaffen tot zijn elektronisch dossier of dat van anderen, kan dit via de behandelende arts laten nagaan. Deze laatste zal, indien nodig, instaan dat de gepaste maatregelen getroffen worden.

5. Sanctionering van inbreuken op de discretieplicht

Diverse interne en externe (bv. strafwetboek) reglementen voorzien maatregelen die kunnen toegepast worden bij ernstige inbreuken op de discretieplicht.

De VZW Mariaziekenhuis zal bovendien niet nalaten de nodige stappen te ondernemen bij inbreuken op de discretieplicht door personen die zich in het kader van hun beroepsuitoefening of hun opleiding binnen de VZW Mariaziekenhuis bewegen, maar geen arbeidsovereenkomst met de VZW Mariaziekenhuis hebben afgesloten.

Handtekening voor ontvangst :
Clerix Emma